Unit E1

# Cosets and normal subgroups

# Introduction to Book E

You met many of the basic ideas of group theory in Book B *Group theory 1*. This book builds on that material and introduces you to more advanced group theory. You will learn more about how group theory reveals links and similarities in concepts that seem unrelated, giving us a greater understanding of these concepts. You will also see examples of how group theory can simplify problems that at first sight appear prohibitively complicated, and so make it possible to solve them.

The mathematics that you will cover in this second group theory book is more abstract than that in the first book, and many students find it more challenging. However, do not let that put you off – being challenged should be an enjoyable part of learning mathematics, and it enables you to meet some quite powerful and beautiful group theory.

To avoid this book being *too* challenging, though, you must make sure that you have a really sound working knowledge of the material covered in the first group theory book, Book B, which forms a foundation for this second book. To help you achieve this, this second book of group theory includes revision of the main ideas and techniques that you will need from the first book. You should work carefully through all the revision material, most of which is in the first unit. Doing this will also give you a useful start on your exam revision.

The ideas that you have already met in Book B are covered much more concisely here than in Book B, so if you find that you need more detail on a topic then you should consult the original coverage of it in Book B. Most of the results from Book B are stated here without proof, as they have already been proved in Book B.

The second unit in this book, Unit E2, is more substantial than the other three units, so you should expect to spend more time studying it.

# Introduction

Sections 1 and 3 of this unit, which together constitute about half of the unit, are devoted to revision of some of the important ideas from Book B. They will give you the grounding that you need before you go on to the more abstract group theory later in the book. These sections also include some interesting examples of groups that you have not met before.

The other three sections cover new topics. Section 2 introduces *matrix groups* – groups whose elements are matrices – which will be used frequently in this book. Section 4 introduces the idea of *cosets*, which are subsets of a group related to a particular subgroup. This work leads in Section 5 to the notion of a *normal subgroup*, which is a crucial concept in group theory: normal subgroups allow us to 'break down' groups into simpler groups. Both cosets and normal subgroups will be important throughout the rest of this book.

# 1 Groups

In this first section you will revise the definition of a group and some basic properties of groups, and go on to revise permutation groups, symmetry groups and subgroups.

## 1.1 Definition of a group

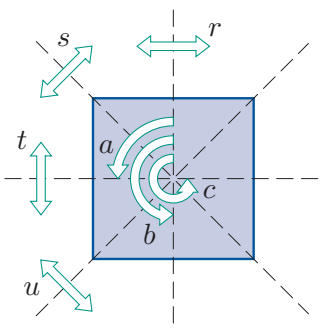



**Figure 1** The symmetries of the square

In mathematics, there are many situations in which we have a set together with a means of combining any two elements of the set. For example, we might have one of the following.

- The set of all real numbers, with addition. We can use addition to combine any two real numbers: for instance, $2.1 + 3.7 = 5.8$.
- The set of all symmetries of the square, with function composition. We can use function composition to combine any two symmetries of the square. For instance, if the symmetries of the square are labelled as shown in Figure 1, then $a \circ b = c$.

A means of combining any two elements of a set is called a **binary operation** defined on the set. If a set and a binary operation defined on the set together possess the four standard properties given in the box below, then the set and binary operation are said to form a *group*.

### Definition

Let $G$ be a set and let $\circ$ be a binary operation defined on $G$. Then $(G, \circ)$ is a **group**, and we also say that $G$ is a **group under** $\circ$, if the following four **group axioms** hold.

**G1 Closure** For all $g$, $h$ in $G$,

$$g \circ h \in G.$$

**G2 Associativity** For all $g$, $h$, $k$ in $G$,

$$g \circ (h \circ k) = (g \circ h) \circ k.$$

**G3 Identity** There is an element $e$ in $G$ such that

$$g \circ e = g = e \circ g \quad \text{for all } g \text{ in } G.$$

(This element is an **identity element** for $\circ$ on $G$.)

**G4 Inverses** For each element $g$ in $G$, there is an element $h$ in $G$ such that

$$g \circ h = e = h \circ g.$$

(The element $h$ is an **inverse element** of $g$ with respect to $\circ$.)

This definition is illustrated in the worked exercise below. When you apply it you may assume without proof that the following binary operations are associative. (You saw that matrix multiplication is associative in Corollary C44 at the end of Subsection 3.1 of Unit C3.)

### Standard associative binary operations

- Addition
- Multiplication
- Modular addition
- Modular multiplication
- Matrix addition
- Matrix multiplication
- Function composition

## Worked Exercise E1

Determine which of the following are groups.

(a) $(\mathbb{Z}, \times)$ (b) $(\mathbb{Z}, +)$

### Solution

(a) We consider each axiom in turn.

To show that a group axiom holds, we must give an algebraic argument that applies to all group elements (though we can assume that axiom G2 holds if the group operation is one of the standard associative binary operations). To show that a group axiom does *not* hold, we must give a counterexample.

**G1 Closure**

For all $m, n \in \mathbb{Z}$,

$$m \times n \in \mathbb{Z},$$

so $\mathbb{Z}$ is closed under multiplication.

**G2 Associativity**

Multiplication of numbers is associative.

**G3 Identity**

We have $1 \in \mathbb{Z}$, and for all $n \in \mathbb{Z}$,

$$n \times 1 = n = 1 \times n.$$

So 1 is an identity element for $\times$ on $\mathbb{Z}$.

**G4 Inverses**

The element 2 is in $\mathbb{Z}$, but it has no inverse with respect to multiplication in $\mathbb{Z}$, since there is no element $n \in \mathbb{Z}$ such that

$$2 \times n = 1 = n \times 2.$$

Thus axiom G4 fails.

Hence $(\mathbb{Z}, \times)$ is not a group.

(b) Again, we consider each axiom in turn.

**G1 Closure**

For all $m, n \in \mathbb{Z}$,

$$m + n \in \mathbb{Z},$$

so $\mathbb{Z}$ is closed under addition.

**G2 Associativity**

Addition of numbers is associative.

**G3 Identity**

We have $0 \in \mathbb{Z}$, and for all $n \in \mathbb{Z}$,

$$n + 0 = n = 0 + n.$$

So 0 is an identity element for $+$ on $\mathbb{Z}$.

**G4 Inverses**

For each $n \in \mathbb{Z}$, we have $-n \in \mathbb{Z}$ and

$$n + (-n) = 0 = -n + n.$$

So each element $n$ in $\mathbb{Z}$ has an inverse element in $\mathbb{Z}$ with respect to addition.

Since all four axioms hold, $(\mathbb{Z}, +)$ is a group.

Although the solution to Worked Exercise E1(a) proceeds by considering all the group axioms systematically until one is found to fail, simply demonstrating that *any one* axiom fails is enough to show that a set and binary operation do not form a group.

## Exercise E1

Let $A = \{5k : k \in \mathbb{Z}\} = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$.

By using the group axioms, determine which of the following are groups.

(a) $(A, +)$ (b) $(A, \times)$

The next exercise involves a group that you have not met before but which will be used later in this book. The binary operation of this group is defined using the idea of the *fractional part* of a real number.

The **fractional part** of a real number $x$, denoted by $\text{frac}(x)$, is given by

$$\text{frac}(x) = x - \lfloor x \rfloor,$$

where $\lfloor x \rfloor$ is the integer part of $x$ (the largest integer that is less than or equal to $x$).

For example,

$$\text{frac}(1.2) = 1.2 - 1 = 0.2,$$
$$\text{frac}(3.9) = 3.9 - 3 = 0.9,$$
$$\text{frac}(5) = 5 - 5 = 0,$$
$$\text{frac}(-2.8) = -2.8 - (-3) = 0.2.$$

Essentially, $\text{frac}(x)$ is equal to 0 if $x$ is an integer, and is equal to the distance from $x$ to 'the next integer down' otherwise, as illustrated in Figure 2. So it is always a number in the interval $[0, 1)$.

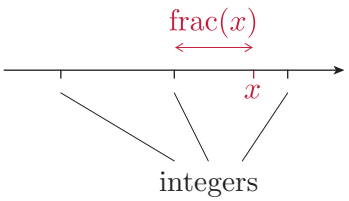



**Figure 2** The fractional part of a real number $x$

The binary operation $+_1$ is defined on the interval $[0, 1)$ by

$$x +_1 y = \text{frac}(x + y).$$

For example,

$$0.9 +_1 0.7 = \text{frac}(0.9 + 0.7) = \text{frac}(1.8) = 0.8.$$

## Exercise E2

Given that the binary operation $+_1$ defined above is associative on the interval $[0, 1)$, show that $\big([0, 1), +_1\big)$ is a group.

(If you want a challenge, try showing also that $+_1$ is associative on $[0, 1)$. A solution to this is provided at the end of the solution to this exercise.)

A group $(G, \circ)$ that has the additional property that

$$g \circ h = h \circ g \quad \text{for all } g, h \text{ in } G$$

is called an **abelian** (or **commutative**) group. A group that is not abelian is **non-abelian**.

The group $(\mathbb{Z}, +)$, from Worked Exercise E1(b), is an example of an abelian group, since $a + b = b + a$ for all $a, b \in \mathbb{Z}$. In fact, any group whose elements are numbers and whose binary operation is addition or multiplication is an abelian group, since $a + b = b + a$ and $a \times b = b \times a$ for all numbers $a$ and $b$. In contrast, a group whose binary operation is function composition or matrix multiplication may be either abelian or non-abelian.

An **infinite** group is one with infinitely many elements. So, for example, the group $(\mathbb{Z}, +)$ is an infinite group. A **finite** group is one with a finite number of elements. If a finite group $(G, \circ)$ has $n$ elements, then we say that it is a group of **order** $n$, and we write $|G| = n$.

The infinite groups of numbers in the box below occur frequently. Remember that $\mathbb{Q}^* = \mathbb{Q} - \{0\}$, $\mathbb{R}^* = \mathbb{R} - \{0\}$ and $\mathbb{C}^* = \mathbb{C} - \{0\}$.

### Some standard infinite groups of numbers

The following are groups:

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +),$$
$$(\mathbb{Q}^*, \times), \quad (\mathbb{R}^*, \times), \quad (\mathbb{C}^*, \times).$$

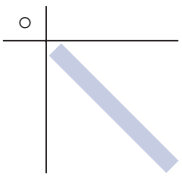



**Figure 3** The main diagonal of a Cayley table

When we are working with a binary operation $\circ$ defined on a small finite set, we often display the composites given by $\circ$ in a **Cayley table**. For each $x$ and $y$ in the set, we enter the composite $x \circ y$ in the Cayley table in the row labelled $x$ and the column labelled $y$. We can use a Cayley table to help us check the group axioms, as described in the box below (recall that the *main diagonal* of a Cayley table is the diagonal shown in Figure 3). The construction of a Cayley table and its use to check the group axioms are demonstrated in the next worked exercise after the box.

### Using a Cayley table to check the group axioms

Let $G$ be a finite set and let $\circ$ be a binary operation defined on $G$. Then $(G, \circ)$ is a group if and only if the Cayley table for $(G, \circ)$ has the following properties.

**G1 Closure** The table contains only elements of the set $G$; that is, no new elements appear in the body of the table.

**G2 Associativity** The operation $\circ$ is associative. (This property is not easy to check from a Cayley table.)

**G3 Identity** A row and a column labelled by the same element repeat the table borders. This element is an identity element, $e$ say.

**G4 Inverses** Each row contains the identity element $e$, occurring either on the main diagonal or symmetrically with another occurrence of $e$, with respect to the main diagonal (see Figure 4). For each such occurrence of $e$, the corresponding elements in the table borders are inverses of each other.

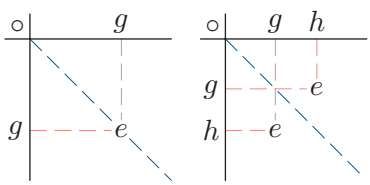



**Figure 4** Occurrences of the identity element indicating inverse elements

Remember also that a finite group is abelian if and only if its Cayley table is symmetric with respect to the main diagonal.

A Cayley table of a group is called a **group table**.

## Worked Exercise E2

Construct a Cayley table for the set $G = \{1, 3, 7, 9\}$ under multiplication modulo 20. Hence show that $(G, \times_{20})$ is a group.

### Solution

The Cayley table is as follows.

| $\times_{20}$ | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 9 | 1 | 7 |
| 7 | 7 | 1 | 9 | 3 |
| 9 | 9 | 7 | 3 | 1 |

We consider each axiom in turn.

**G1 Closure**

Every element in the body of the table is in $G$, so $G$ is closed under $\times_{20}$.

**G2 Associativity**

Modular multiplication is associative.

**G3 Identity**

We look for a row and column with the same label that repeat the table borders.

The table shows that 1 is an identity element for $\times_{20}$ on $G$.

**G4 Inverses**

We check that each row contains the identity element 1, either on the main diagonal or symmetrically with respect to it.

The table shows that 1 and 9 are self-inverse, and 3 and 7 are inverses of each other.

Since all four axioms hold, $(G, \times_{20})$ is a group.

Remember that a **self-inverse** element is one that is an inverse of itself. In a Cayley table each self-inverse element corresponds to an occurrence of the identity element $e$ on the main diagonal, as shown in Figure 5.

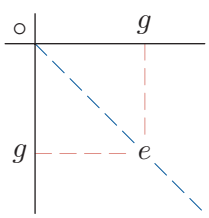



**Figure 5** A self-inverse element $g$

## Exercise E3

Let $G = \{\mathbf{I}, \mathbf{R}, \mathbf{S}, \mathbf{T}\}$ where

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{R} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{S} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}, \ \mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Construct a Cayley table for the set $G$ under matrix multiplication. Hence show that $(G, \times)$ is a group. Determine whether it is an abelian group.

(Notice that $\mathbf{I}$, $\mathbf{R}$, $\mathbf{S}$ and $\mathbf{T}$ are all diagonal matrices and hence are straightforward to multiply together.)

In the next exercise you will need to construct Cayley tables using modular arithmetic. Remember that there are ways to make modular arithmetic calculations quicker and easier, as you saw in Subsection 3.3 of Unit A2 *Number systems*. For example, to work out $9 \times_{24} 15$, instead of starting by working out $9 \times 15 = 135$, you can proceed as follows:

$$\begin{aligned} 9 \times 15 &\equiv 9 \times 3 \times 5 \\ &\equiv 27 \times 5 \\ &\equiv 3 \times 5 \\ &\equiv 15 \pmod{24}. \end{aligned}$$

Thus $9 \times_{24} 15 = 15$.

Similarly, to work out $9 \times_{24} 21$, you can proceed as follows:

$$\begin{aligned} 9 \times 21 &\equiv 9 \times (-3) \\ &\equiv -27 \\ &\equiv -3 \\ &\equiv 21 \pmod{24}. \end{aligned}$$

Thus $9 \times_{24} 21 = 21$.

You can also make use of the fact that modular addition and modular multiplication are commutative binary operations, so a Cayley table for a set of numbers with one of these operations will be symmetric with respect to its main diagonal.

## Exercise E4

In each of the following cases, construct a Cayley table for the set and binary operation, and hence determine whether they form a group.

(a) $(\{0, 1, 2\}, +_3)$ (b) $(\{2, 4, 6\}, \times_8)$ (c) $(\{1, 5\}, \times_6)$

(d) $(\{3, 9, 15, 21\}, \times_{24})$

Exercise E4(a) and (c) are particular examples of the first two of the following general results that you met in Unit B1 *Symmetry and groups*. (Here and elsewhere in this book, results from Book B are quoted with their original numbers.)

### Standard finite groups of numbers

**Theorem B8** For each integer $n \geq 2$, the set $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ is a group under $+_n$.

**Theorem B9** For each integer $n \geq 2$, the set $U_n$ of all integers in $\mathbb{Z}_n$ that are coprime to $n$ is a group under $\times_n$.

**Corollary B10** For each prime $p$, the set $\mathbb{Z}_p^* = \{1, 2, \ldots, p-1\}$ is a group under $\times_p$. (Note that $U_p = \mathbb{Z}_p^*$ when $p$ is prime.)

## Exercise E5

List the elements of each of the following groups.

(a) $(U_{18}, \times_{18})$ (b) $(U_7, \times_7)$ (c) $(\mathbb{Z}_7^*, \times_7)$

In Unit B1 you met some useful facts that follow directly from the group axioms. Here is an important one to remember, from Subsection 4.1 of Unit B1.

In a group $(G, \circ)$ we write composites of three or more elements such as $g \circ h \circ k$ and $g \circ h \circ k \circ l$ without brackets, because it follows from axiom G2 that any possible way of interpreting such a composite gives the same answer.

For example, the composite $g \circ h \circ k$ can be evaluated by interpreting it as either $g \circ (h \circ k)$ or $(g \circ h) \circ k$. It does not matter which of these expressions we choose, as they both give the same answer, by axiom G2.

Remember, though, that in general we cannot change the *order* of the elements in a composite of group elements. For example, $g \circ h \circ k$ is not necessarily equal to $h \circ g \circ k$. However, if the group is abelian, then we *can* change the order of the elements in a composite in any way we like, since all possible orders will give the same answer.

The two boxes below contain some other important results about groups that follow directly from the group axioms.

### Uniqueness of the identity and of inverses

The following hold in any group.

**Proposition B11** The identity element is unique. We usually denote it by $e$.

**Proposition B12** Each element $x$ has a unique inverse. We usually denote it by $x^{-1}$.

### Basic properties of group elements

The following hold for any elements $x$, $y$, $a$ and $b$ of any group $(G, \circ)$.

**Proposition B13** $(x^{-1})^{-1} = x$

**Proposition B14** $(x \circ y)^{-1} = y^{-1} \circ x^{-1}$

**Proposition B15** **Left and Right Cancellation Laws**

If $x \circ a = x \circ b$, then $a = b$.

If $a \circ x = b \circ x$, then $a = b$.

You saw in Unit B1 that the Left and Right Cancellation Laws can be used to prove the following property of group tables.

**Proposition B18**

In a group table, each element of the group occurs exactly once in each row and exactly once in each column.

Thus, if you meet a Cayley table in which this property does not hold, then you can immediately conclude that it is not a group table. For example, if the set $\{e, a, b, c\}$ with binary operation $\circ$ has the Cayley table

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $e$ | $c$ | $b$ |
| $b$ | $b$ | $c$ | $b$ | $e$ |
| $c$ | $c$ | $b$ | $e$ | $b$ |

then $(\{e, a, b, c\}, \circ)$ is not a group because $b$ occurs more than once and $a$ not at all in some rows and columns of the Cayley table.

It is important to remember that a group $(G, \circ)$ consists of *two* things: the set $G$ and the binary operation $\circ$. However, frequently for convenience we refer to a group $(G, \circ)$ just as the group $G$, provided this will not cause confusion. For instance, we often do this in the following situations:

- where there is an 'obvious' binary operation under which a set $G$ is a group
- where the binary operation associated with a set $G$ is clear from the context
- where we are discussing a general, abstract group and do not need to refer to the binary operation.

For example, we might refer to the group $(\mathbb{R}^*, \times)$ simply as 'the group $\mathbb{R}^*$', since the only obvious binary operation under which $\mathbb{R}^*$ is a group is multiplication.

## 1.2 Permutation groups

An important family of groups is that of groups of *permutations*.
A **permutation** of a finite set $S$ is a one-to-one function from $S$ to $S$. It can be written in **two-line form**. For example, the notation

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 2 & 1 & 4 \end{pmatrix}$$

specifies that the permutation $f$ maps 1 to 5, 2 to 6, 3 to 3, and so on.

A more convenient notation for permutations is **cycle form**. This notation depends on the fact that for any permutation $f$ of a set $S$, if we write down all the elements of $S$ and draw an arrow from each element to its image under $f$, then we obtain one or more **cycles**. For example, if we do this for the permutation $f$ above, then we obtain the cycles shown in Figure 6.

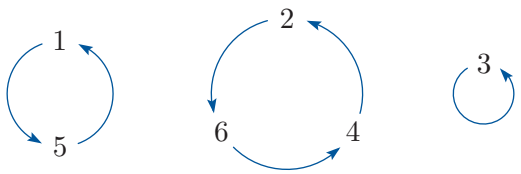



**Figure 6** The cycles of the permutation $f$

Using these cycles, we write the permutation $f$ above in cycle form as

$$f = (1\ 5)(2\ 6\ 4)(3).$$

In the cycle form of a permutation, each cycle can be written with any of its symbols as the first symbol, and the cycles can be written in any order. For example, an alternative way to write the permutation $f$ above is

$$f = (3)(6\ 4\ 2)(5\ 1).$$

However, if the symbols in the permutation are numbers then we usually write the smallest symbol in each cycle first and arrange the cycles with their smallest symbols in increasing order, unless there is a reason to do otherwise.

The **length** of a cycle is the number of symbols in it, and a cycle of length $r$ is called an **$r$-cycle**. We usually omit 1-cycles from the cycle form of a permutation. So our standard way to write the permutation $f$ above is

$$f = (1\ 5)(2\ 6\ 4).$$

Note that the cycles in the cycle form of a permutation are **disjoint** – that is, they have no elements in common.

Any two permutations of the same set $S$ can be composed to give another permutation of $S$. For example, if $f$ is the permutation $(1\ 5)(2\ 6\ 4)$ above and $g$ is the permutation $(1\ 5\ 4\ 3\ 6)$, then the composite $g \circ f$ (that is, $f$ followed by $g$) can be illustrated as follows.

| | | | | | | |
|---|---|---|---|---|---|---|
| | 1 | 2 | 3 | 4 | 5 | 6 |
| $f$ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| | 5 | 6 | 3 | 2 | 1 | 4 |
| $g$ | ↓ | ↓ | ↓ | ↓ | ↓ | ↓ |
| | 4 | 1 | 6 | 2 | 5 | 3 |

This diagram shows, for example, that $f$ maps 1 to 5 and then $g$ maps 5 to 4, so altogether $g \circ f$ maps 1 to 4.

The worked exercise below demonstrates how to compose two permutations by directly using their cycle forms, for the same two permutations $f$ and $g$ as above.

## Worked Exercise E3

Find, in cycle form, the composite permutation $g \circ f$ of the permutations

$$f = (1\ 5)(2\ 6\ 4) \quad \text{and} \quad g = (1\ 5\ 4\ 3\ 6).$$

### Solution

We start a cycle of $g \circ f$ with the smallest symbol, 1. The permutation $f$ maps 1 to 5 and then $g$ maps 5 to 4, so $g \circ f$ maps 1 to 4.

$$g \circ f = (1\ 5\ 4\ 3\ 6) \circ (1\ 5)(2\ 6\ 4) = (1\ 4\ \ldots$$

To continue the cycle, we find the image of 4. The permutation $f$ maps 4 to 2 and $g$ fixes 2, so $g \circ f$ maps 4 to 2.

$$= (1\ 4\ 2\ \ldots$$

Continuing in this way, we find that $g \circ f$ maps 2 to 1, completing the cycle.

$$= (1\ 4\ 2)\ldots$$

We start the next cycle with the smallest symbol whose image under $g \circ f$ we have not yet found, and continue in a similar way until we have included all the symbols.

$$g \circ f = (1\ 5\ 4\ 3\ 6) \circ (1\ 5)(2\ 6\ 4) = (1\ 4\ 2)(3\ 6)(5) = (1\ 4\ 2)(3\ 6)$$

Remember that the order in which you compose permutations is important: if $f$ and $g$ are permutations, then the composite $f \circ g$ may not be equal to the composite $g \circ f$.

## Exercise E6

Determine the cycle form of each of the following composites of permutations.

(a) $(1\ 2\ 7\ 5)(3\ 8\ 4) \circ (1\ 3\ 6\ 7\ 5)$ (b) $(1\ 3\ 7)(2\ 5\ 4) \circ (2\ 4)(3\ 8)(5\ 6)$

You can use the method demonstrated in Worked Exercise E3 to compose any number of permutations. For example, in Exercise E7 (below) the first (right-most) permutation maps 1 to 7, then the next permutation maps 7 to 4, and finally the third permutation maps 4 to 5, so altogether 1 is mapped to 5.

## Exercise E7

Determine the cycle form of the following composite of permutations.

$$(1\ 4\ 5\ 6) \circ (2\ 3\ 7\ 4\ 8) \circ (1\ 7\ 6)(3\ 2\ 5).$$

Any permutation is equal to the composite (in any order) of its disjoint cycles. For example,

$$(1\ 5)(2\ 6\ 4) = (1\ 5) \circ (2\ 6\ 4) = (2\ 6\ 4) \circ (1\ 5).$$

However, not every composite of cycles can be interpreted as the cycle form of a permutation. For example, $(1\ 2) \circ (2\ 3)$ is a composite of cycles, but $(1\ 2)(2\ 3)$ is not the cycle form of a permutation because the two cycles here are *not disjoint* (they have the symbol 2 in common).

The inverse of a permutation of a set $S$ is another permutation of $S$. For example, if $f = (1\ 5)(2\ 6\ 4)$, as above, then the effect of $f$ is

$$f: \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\ 5 & 6 & 3 & 2 & 1 & 4 \end{array},$$

so the effect of its inverse $f^{-1}$, obtained by reversing the arrows, is

$$f^{-1}: \begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \uparrow & \uparrow & \uparrow & \uparrow & \uparrow & \uparrow \\ 5 & 6 & 3 & 2 & 1 & 4 \end{array}.$$

The next worked exercise demonstrates how to find the inverse of a permutation directly from its cycle form.

## Worked Exercise E4

Find, in cycle form, the inverse of the permutation $f = (1\ 5)(2\ 6\ 4)$.

### Solution

We simply reverse all the cycles.

$$f^{-1} = (5\ 1)(4\ 6\ 2)$$

We then write $f^{-1}$ in the usual form, with the smallest symbol in each cycle first.

$$= (1\ 5)(2\ 4\ 6)$$

## Exercise E8

Find the inverse of each of the following permutations.

(a) $(1\ 7\ 5\ 2)(3\ 8\ 4)$ (b) $(1\ 4)(2\ 3)(6\ 8)$

The technique of reversing the cycles to find the inverse of a permutation works *only if the permutation is in cycle form*. For example, the inverse of the composite permutation $(1\ 2\ 3) \circ (3\ 4)$ is *not* obtained by reversing the cycles $(1\ 2\ 3)$ and $(3\ 4)$, because these cycles are not disjoint.

A 2-cycle is called a **transposition**. Any cycle can be expressed as a composite of transpositions, as follows.

### Strategy B10

To express a cycle $(a_1\ a_2\ a_3\ \ldots\ a_r)$ as a composite of transpositions, write the transpositions

$$(a_1\ a_2),\ (a_1\ a_3),\ (a_1\ a_4),\ \ldots,\ (a_1\ a_r)$$

in reverse order and form their composite. That is,

$$(a_1\ a_2\ a_3\ \ldots\ a_r) = (a_1\ a_r) \circ (a_1\ a_{r-1}) \circ \cdots \circ (a_1\ a_3) \circ (a_1\ a_2).$$

For example, as you can check by composing the transpositions,

$$(1\ 2\ 3\ 4\ 5\ 6) = (1\ 6) \circ (1\ 5) \circ (1\ 4) \circ (1\ 3) \circ (1\ 2).$$

Because any cycle can be expressed as a composite of transpositions, so can any permutation, as illustrated in the next worked exercise.

## Worked Exercise E5

Write the permutation $(1\ 5\ 7\ 2)(3\ 4\ 6)$ as a composite of transpositions.

### Solution

Use Strategy B10 to write each cycle in the permutation as a composite of transpositions.

$$(1\ 5\ 7\ 2)(3\ 4\ 6) = (1\ 2) \circ (1\ 7) \circ (1\ 5) \circ (3\ 6) \circ (3\ 4)$$

## Exercise E9

Write the permutation $(1\ 5\ 3)(2\ 4\ 7\ 9\ 6)$ as a composite of transpositions.

There are many different ways to express a particular permutation as a composite of transpositions. For example, by Strategy B10 the permutation (3 4 5) can be written as

$$(3\ 5) \circ (3\ 4),$$

but since (3 4 5) = (4 5 3), it can also be written as

$$(4\ 3) \circ (4\ 5).$$

A third way to write it is

$$(3\ 5) \circ (3\ 4) \circ (1\ 2) \circ (1\ 2),$$

since (1 2) is the inverse of itself.

However, we have the following theorem.

### Theorem B58 Parity Theorem

A permutation cannot be expressed both as a composite of an even number of transpositions and as a composite of an odd number of transpositions.

We say that a permutation is **even** if it can be expressed as a composite of an even number of transpositions, and **odd** if it can be expressed as a composite of an odd number of transpositions. The evenness or oddness of a permutation is called its **parity**.

The parity of a permutation has the properties in the box below.

The first two properties come from the fact that an $r$-cycle can be expressed as a composite of $r - 1$ transpositions, by Strategy B10. The third and fourth properties come from considering the numbers of transpositions in composites of permutations.

### Properties of the parity of a permutation

- A cycle of odd length is an even permutation.
- A cycle of even length is an odd permutation.
- The composite of two odd or two even permutations is even.
- The composite of an even and an odd permutation is odd.

We can use these four properties to determine the parity of any permutation expressed in cycle form, as demonstrated in the following worked exercise.

## Worked Exercise E6

Determine the parity of the permutation

$$f = (1\ 3\ 4)(2\ 6)(5\ 9\ 7\ 8).$$

### Solution

The cycles (1 3 4), (2 6) and (5 9 7 8) are even, odd and odd, respectively. Hence the permutation $f$ is

$$\text{even} + \text{odd} + \text{odd} = \text{even}.$$

## Exercise E10

Determine the parity of each of the following permutations.

(a) $(1\ 5\ 8)(2\ 7\ 3\ 4)$ (b) $(1\ 8)(2\ 7)(3\ 5\ 4\ 6)$

The method of determining parity demonstrated in Worked Exercise E6 shows us that any two permutations with the same **cycle structure** (that is, the same number of cycles of each length) have the same parity. For example, the permutations (1 2)(3 4 6) and (1 4 3)(2 5) have the same cycle structure and hence the same parity.

In Unit B3 *Permutations* you saw proofs of the following facts.

### The symmetric group $S_n$ and the alternating group $A_n$

**Theorems B52 and B53** For each positive integer $n$, the set $S_n$ of all permutations of the set $\{1, 2, \ldots, n\}$ is a group under function composition, called the **symmetric group of degree** $n$. It has order $n!$.

**Theorems B61 and B62** For each positive integer $n$, the set $A_n$ of all even permutations of the set $\{1, 2, \ldots, n\}$ is a group under function composition, called the **alternating group of degree** $n$. For $n \geq 2$ it has order $\frac{1}{2}n!$.

The identity element of both the group $S_n$ and the group $A_n$ is the permutation that maps every element of the set $\{1, 2, \ldots, n\}$ to itself, which we call the **identity permutation** and usually denote by $e$. The group $S_n$ is non-abelian for $n \geq 3$ and the group $A_n$ is non-abelian for $n \geq 4$.

The group $A_n$ is a *subgroup* of the group $S_n$: you will revise the idea of a subgroup in Subsection 1.4.

A group whose elements are permutations of a finite set and whose binary operation is function composition is called a **permutation group**.

## 1.3 Symmetry groups

A rich source of examples of groups, many of them non-abelian, is the symmetry of figures. A **figure** in $\mathbb{R}^2$ is any subset of $\mathbb{R}^2$, such as a triangle, a square, a rectangle or a line. Similarly, a **figure** in $\mathbb{R}^3$ is any subset of $\mathbb{R}^3$, such as a tetrahedron or a cuboid. Some examples of figures are shown in Figure 7. A figure in $\mathbb{R}^2$ is called a **plane figure**. A figure in $\mathbb{R}^3$ is called a **solid figure** if it has non-zero height, non-zero width and non-zero depth.

**Figure 7** Examples of plane and solid figures

An **isometry** of $\mathbb{R}^2$ is a function $f : \mathbb{R}^2 \longrightarrow \mathbb{R}^2$ that preserves distances; that is, for all points $X, Y \in \mathbb{R}^2$, the distance between $f(X)$ and $f(Y)$ is the same as the distance between $X$ and $Y$. A **symmetry** of a plane figure is an isometry of $\mathbb{R}^2$ that maps the figure to itself. An isometry of $\mathbb{R}^3$, and a symmetry of a 3-dimensional figure, are defined in an analogous way.

It is straightforward to check that the set of symmetries of a figure, with the binary operation of function composition, satisfies the group axioms: try thinking this through for yourself. So we have the following theorem.

### Theorem B21

If $F$ is a figure (in $\mathbb{R}^2$ or $\mathbb{R}^3$), then the set $S(F)$ of all symmetries of $F$ is a group under function composition, called the **symmetry group** of $F$.

For example, you have met $S(\triangle)$, $S(\square)$, $S(\rectangle)$ and $S(\hexagon)$, the symmetry groups of the equilateral triangle, the square, the rectangle and the regular hexagon, with orders 6, 8, 4 and 12, respectively. You have also met $S(\text{tet})$ and $S(\text{cuboid})$, the symmetry groups of the regular tetrahedron and a cuboid with no square faces, with orders 24 and 8, respectively.

The identity element of the symmetry group of a figure $F$ is called the **identity symmetry** of $F$, and is usually denoted by $e$.

The groups $S(\triangle)$, $S(\square)$ and $S(\rectangle)$ are summarised below. Figures 8, 9 and 10 show the elements of these groups, except the identity symmetry, and Tables 1, 2 and 3 describe these elements. Each element can be represented as a permutation of the labels of the vertex locations, as given in the tables. For example, the symmetry $a$ of the equilateral triangle is represented by the permutation (1 2 3) because it maps the vertex at location 1 to the vertex at location 2, the vertex at location 2 to the vertex at location 3, and the vertex at location 3 to the vertex at location 1. Remember that the numbers label the vertex *locations* rather than the vertices themselves: the labels do not move when the figure is transformed by a symmetry.

Here and throughout the group theory units we express angles of rotation of plane figures in radians *anticlockwise*, unless otherwise stated.

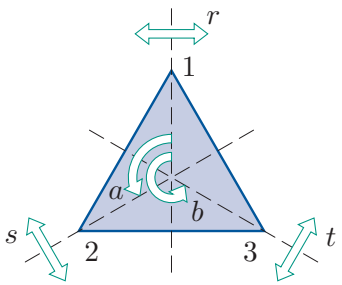



**Figure 8** $S(\triangle)$

**Table 1** The elements of $S(\triangle)$

| Symmetry | Description | Representation |
|---|---|---|
| $e$ | identity | $e$ |
| $a$ | rotation though $2\pi/3$ | (1 2 3) |
| $b$ | rotation though $4\pi/3$ | (1 3 2) |
| $r$ | reflection in axis through vertex 1 | (2 3) |
| $s$ | reflection in axis through vertex 2 | (1 3) |
| $t$ | reflection in axis through vertex 3 | (1 2) |

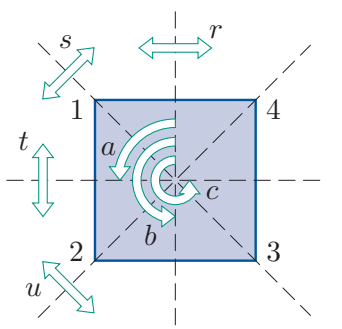



**Figure 9** $S(\square)$

**Table 2** The elements of $S(\square)$

| Symmetry | Description | Representation |
|---|---|---|
| $e$ | identity | $e$ |
| $a$ | rotation through $\pi/2$ | (1 2 3 4) |
| $b$ | rotation through $\pi$ | (1 3)(2 4) |
| $c$ | rotation through $3\pi/2$ | (1 4 3 2) |
| $r$ | reflection in vertical axis | (1 4)(2 3) |
| $s$ | reflection in diagonal through vertex 1 | (2 4) |
| $t$ | reflection in horizontal axis | (1 2)(3 4) |
| $u$ | reflection in diagonal through vertex 2 | (1 3) |

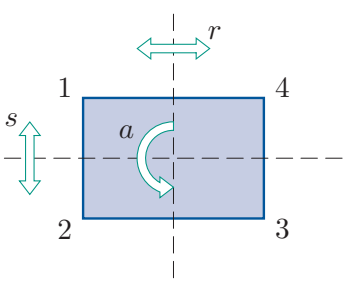



**Figure 10** $S(\square)$

**Table 3** The elements of $S(\square)$

| Symmetry | Description | Representation |
|---|---|---|
| $e$ | identity | $e$ |
| $a$ | rotation through $\pi$ | (1 3)(2 4) |
| $r$ | reflection in vertical axis | (1 4)(2 3) |
| $s$ | reflection in horizontal axis | (1 2)(3 4) |

We can compose the symmetries of a figure by composing the permutations that represent them. For example, for the symmetries $s$ and $b$ in $S(\triangle)$ we have

$$b \circ s = (1\ 3\ 2) \circ (1\ 3) = (1\ 2)(3) = (1\ 2) = t.$$

By combining all pairs of symmetries in each of $S(\triangle)$, $S(\square)$ and $S(\rectangle)$ in this way, we obtain the following group tables.

| $\circ$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
| $a$ | $a$ | $b$ | $e$ | $t$ | $r$ | $s$ |
| $b$ | $b$ | $e$ | $a$ | $s$ | $t$ | $r$ |
| $r$ | $r$ | $s$ | $t$ | $e$ | $a$ | $b$ |
| $s$ | $s$ | $t$ | $r$ | $b$ | $e$ | $a$ |
| $t$ | $t$ | $r$ | $s$ | $a$ | $b$ | $e$ |

$S(\triangle)$

| $\circ$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
| $a$ | $a$ | $b$ | $c$ | $e$ | $s$ | $t$ | $u$ | $r$ |
| $b$ | $b$ | $c$ | $e$ | $a$ | $t$ | $u$ | $r$ | $s$ |
| $c$ | $c$ | $e$ | $a$ | $b$ | $u$ | $r$ | $s$ | $t$ |
| $r$ | $r$ | $u$ | $t$ | $s$ | $e$ | $c$ | $b$ | $a$ |
| $s$ | $s$ | $r$ | $u$ | $t$ | $a$ | $e$ | $c$ | $b$ |
| $t$ | $t$ | $s$ | $r$ | $u$ | $b$ | $a$ | $e$ | $c$ |
| $u$ | $u$ | $t$ | $s$ | $r$ | $c$ | $b$ | $a$ | $e$ |

$S(\square)$

| $\circ$ | $e$ | $a$ | $r$ | $s$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $r$ | $s$ |
| $a$ | $a$ | $e$ | $s$ | $r$ |
| $r$ | $r$ | $s$ | $e$ | $a$ |
| $s$ | $s$ | $r$ | $a$ | $e$ |

$S(\rectangle)$

## Exercise E11

Use the group table for $S(\triangle)$ to determine the following.

(a) $a \circ s$ (b) $b^{-1}$ (c) $b \circ r \circ a$

*Hint*: In part (c), write $b \circ r \circ a$ as either $b \circ (r \circ a)$ or $(b \circ r) \circ a$.

A symmetry of a plane figure is **direct** if its effect can be demonstrated using a model of the figure without removing the model from the plane. For a solid figure, a symmetry is **direct** if its effect can be demonstrated directly in space using a model of the figure. The symmetries of a plane or solid figure that are not direct are called **indirect**.

If a plane figure is bounded, then its direct symmetries are rotations about a central point (including the identity symmetry, which is a rotation through 0 radians), and its indirect symmetries, if it has any, are reflections in lines through this point. For example, in $S(\triangle)$, the direct symmetries are $e$, $a$ and $b$, and the indirect symmetries are $r$, $s$ and $t$.

If a solid figure is bounded, then its direct symmetries are rotations about lines, and its indirect symmetries, if it has any, include reflections in planes and possibly other types of indirect symmetries.

### Properties of direct and indirect symmetries

- The composite of two direct symmetries or two indirect symmetries is direct.
- The composite of a direct symmetry and an indirect symmetry is indirect.

**Theorem B22** If a figure has a finite number of symmetries, then either they are all direct or half are direct and half are indirect.

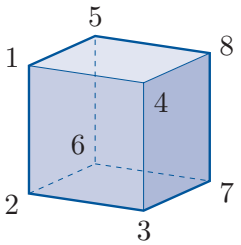



**Figure 11** The cube

The symmetries of a solid figure can be represented by permutations of its vertex location labels in the same way as those of a plane figure. For example, if the vertex locations of the cube are labelled as shown in Figure 11, then the reflection in the horizontal plane through the centre of the cube is represented by the permutation $(1\ 2)(3\ 4)(5\ 6)(7\ 8)$.

For brevity, from now on in this book we will use phrases such as 'vertex labels', rather than the more correct 'labels of the vertex locations', and 'the line 14', rather than the more correct 'the line through the vertices at locations 1 and 4'.

### Exercise E12

This question is about the labelled cube in Figure 11.

(a) Describe geometrically the symmetry of the cube represented by each of the following permutations.

(i) $(1\ 8)(2\ 7)$ (ii) $(1\ 4\ 8\ 5)(2\ 3\ 7\ 6)$

(b) Compose the two permutations in part (a) in each of the two possible orders, and describe geometrically the symmetry represented by each of the resulting two composite symmetries.

(c) Write down, in cycle form, the permutation that represents each of the following symmetries of the cube.

(i) Rotation through $\pi$ about the line that passes through the midpoints of the faces 1265 and 4378.

(ii) The two non-trivial rotations about the line that passes through the vertices 1 and 7.

## 1.4 Subgroups

We make the following definition.

### Definition

A **subgroup** of a group $(G, \circ)$ is a group $(H, \circ)$, where $H$ is a subset of $G$.

Notice that for a group $H$ to be a subgroup of a group $G$ the binary operation must be the *same* for $G$ and $H$.

For example, the group $(\mathbb{Q}, +)$ is a subgroup of the group $(\mathbb{R}, +)$, since $\mathbb{Q}$ is a subset of $\mathbb{R}$ and the two groups have the same binary operation. On the other hand, the group $(\mathbb{R}^*, \times)$ is not a subgroup of the group $(\mathbb{R}, +)$, even though $\mathbb{R}^*$ is a subset of $\mathbb{R}$, because the two groups do not have the same binary operation.

Every group of order greater than 1 has at least two subgroups, namely the group itself and the **trivial subgroup**, whose only element is the identity element.

The following two theorems were proved in Unit B2 *Subgroups and isomorphisms*.

### Theorem B23 Identity and inverses in a subgroup

Let $(G, \circ)$ be a group with a subgroup $(H, \circ)$.

(a) The identity element of $(H, \circ)$ is the same as the identity element of $(G, \circ)$.

(b) For each element $h$ of $H$, the inverse of $h$ in $(H, \circ)$ is the same as its inverse in $(G, \circ)$.

### Theorem B24 Subgroup test

Let $(G, \circ)$ be a group with identity element $e$, and let $H$ be a subset of $G$. Then $(H, \circ)$ is a subgroup of $(G, \circ)$ if and only if the following three properties hold.

**SG1 Closure** For all $x$, $y$ in $H$, the composite $x \circ y$ is in $H$.

**SG2 Identity** The identity element $e$ of $G$ is in $H$.

**SG3 Inverses** For each $x$ in $H$, its inverse $x^{-1}$ in $G$ is in $H$.

We refer to properties SG1, SG2 and SG3 as the three **subgroup properties**. Subgroup property SG1 (closure) is the same as group axiom G1 (closure). However, subgroup properties SG2 (identity) and SG3 (inverses) are not the same as group axioms G3 (identity) and G4 (inverses): these two subgroup properties are concerned with *belonging to*, whereas the corresponding two group axioms are concerned with *existence*.

Notice that before you check the three subgroup properties for a subset $H$ of a group $G$, you first have to be sure that $H$ is a *subset* of $G$, and that the binary operation $\circ$ defined on $H$ is the same as that defined on $G$. If either of these conditions do not hold, then $(H, \circ)$ cannot be a subgroup of $(G, \circ)$.

For a *finite* subset of a group, if you suspect that the subset *is* a subgroup, then it can be helpful to construct a Cayley table for the subset before you try to apply Theorem B24. In the next exercise you can practise applying Theorem B24 to finite subsets of a group.

## Exercise E13

Determine whether each of the following sets, with the binary operation $\times_{25}$, is a subgroup of the group $(U_{25}, \times_{25})$.

(Remember that $U_{25}$ is the set of integers in $\mathbb{Z}_{25}$ coprime to 25.)

(a) $A = \{1, 5, 10, 15, 20\}$ (b) $B = \{1, 6, 11, 16, 21\}$

(c) $C = \{1, 9, 11, 21\}$

As with groups in general, we often refer to a subgroup $(H, \circ)$ of a group $(G, \circ)$ simply as the subgroup $H$ if the binary operation is clear from the context. This is done in the solution to Exercise E13. Also, if you are asked to show that a particular subset $H$ of a group $G$ is a subgroup of $G$, then you should assume that the binary operation on $H$ is the same as on $G$.

## Exercise E14

Let $x$ be a self-inverse element of a group $(G, \circ)$ with identity $e$. Show that $\{e, x\}$ is a subgroup of $G$.

You will have an opportunity to practise applying Theorem B24 to infinite subsets of infinite groups in the next section. In the rest of this subsection we will look briefly at some subsets of particular types of finite groups, namely symmetry groups and symmetric groups. We will also revise Lagrange's Theorem, which is about subgroups of finite groups.

### Subgroups of symmetry groups

In Unit B2 you met the following result.

**Theorem B25**

Let $F$ be a figure in $\mathbb{R}^2$ or $\mathbb{R}^3$. Then the set of direct symmetries of $F$, denoted by $S^+(F)$, is a subgroup of the symmetry group $S(F)$ of $F$.

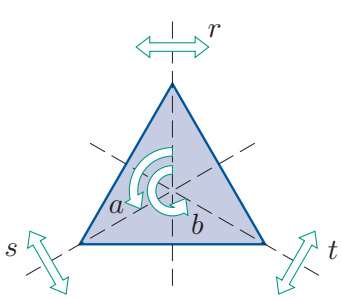



**Figure 12** $S(\triangle)$

For example, the set $S^+(\triangle) = \{e, a, b\}$ of direct symmetries of the equilateral triangle is a subgroup of $S(\triangle)$. (The non-identity elements of $S(\triangle)$ are shown in Figure 12.)

You also saw that you can find subgroups of a symmetry group $S(F)$ by modifying the figure $F$. For example, the plane figure in Figure 13 is a modified version of the equilateral triangle in Figure 12. The only symmetries of the original triangle that are also symmetries of the modified triangle are $e$ and $r$, so $\{e, r\}$ is a subgroup of $S(\triangle)$.

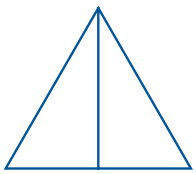


**Figure 13** A modified equilateral triangle

Table 4 lists all the subgroups of the group $S(\triangle)$: there are six altogether. The three subgroups of order 2 can be obtained by modifying the triangle in ways similar to that shown in Figure 13. Alternatively, we can use the fact that if $x$ is any self-inverse element in a group $G$ with identity $e$, then $\{e, x\}$ is a subgroup of $G$, as shown in the solution to Exercise E14. The three elements $r$, $s$ and $t$ of $S(\triangle)$ are all self-inverse.

**Table 4** The subgroups of $S(\triangle)$

| Order | Number of subgroups | Subgroups |
|---|---|---|
| 1 | 1 | $\{e\}$ |
| 2 | 3 | $\{e, r\}$, $\{e, s\}$, $\{e, t\}$ |
| 3 | 1 | $\{e, a, b\}$ |
| 6 | 1 | $S(\triangle)$ |

## Exercise E15

The non-identity elements of the symmetry group $S(\square)$ are shown in Figure 14. The group $S(\square)$ has ten subgroups:

(a) one subgroup of order 1

(b) five subgroups of order 2

(c) three subgroups of order 4

(d) one subgroup of order 8.

Write down as many of these subgroups as you can. (Do not look back to where these subgroups are given in Book B!)

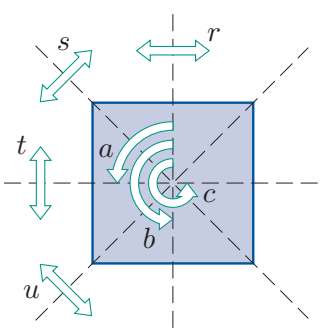



**Figure 14** $S(\square)$

## Subgroups of symmetric groups

In Unit B3 you met various subgroups of symmetric groups. Each symmetric group $S_n$ has the alternating group $A_n$ as a subgroup, as mentioned in Subsection 1.3.

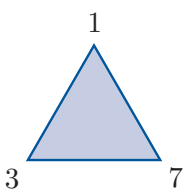
One way to find another subgroup of a symmetric group $S_n$ is to draw a suitable figure, label its vertices (or some other suitable features, such as its edges) with some or all of the symbols from the set $\{1, 2, \ldots, n\}$, and represent the symmetries of the figure as permutations of these labels. For example, the labelled rectangle in Figure 15 gives the following subgroup of $S_6$:

$$\{e, (1\ 3)(4\ 6), (1\ 6)(3\ 4), (1\ 4)(3\ 6)\}.$$


**Figure 15** A labelled rectangle

### Exercise E16

Use the labelled figure below to find a subgroup of the symmetric group $S_7$.




Another way to find a subgroup of a symmetric group $S_n$ is to find all the permutations in $S_n$ that fix a particular symbol from the set $\{1, 2, \ldots, n\}$, or that fix each symbol in some set of symbols. For example, $\{e, (1\ 4)\}$ is the subgroup of $S_4$ whose elements are the permutations in $S_4$ that fix the symbols in the set $\{2, 3\}$.

There are many more ways to find a subgroup of a symmetric group. Another way is given in the next exercise.

### Exercise E17

(a) Let $n$ be a positive integer and let $A$ be any subset of the set $S = \{1, 2, \ldots, n\}$. Let $G$ be the subset of the symmetric group $S_n$ that consists of all the permutations in $S_n$ that map each element of $A$ to another element of $A$. By using Theorem B24 (Subgroup test), prove that $G$ is a subgroup of $S_n$.

(b) List the elements of the group $G$ defined in part (a) when $n = 5$ and $A = \{4, 5\}$.

### Lagrange's Theorem

The following fundamental theorem was proved in Unit B4 *Lagrange's Theorem and small groups*.

**Theorem B68 Lagrange's Theorem**

Let $G$ be a finite group and let $H$ be any subgroup of $G$. Then the order of $H$ divides the order of $G$.

The converse of Lagrange's Theorem is *not* true. In other words, if $m$ is a positive divisor of the order of a group $G$, then there is no guarantee that $G$ has a subgroup of order $m$. It may have such a subgroup, or it may not.

# 2 Matrix groups

Unlike Sections 1 and 3, this section does not contain revision of group theory that you have already met in Book B. It is about a new topic: matrix groups.

In Subsections 3.1 and 4.1 of Unit C1 *Linear equations and matrices* you saw that, for any positive integers $m$ and $n$,

- the set of all $m \times n$ matrices with real entries forms a group under matrix addition, denoted by $M_{m,n}$
- the set of all *invertible* $n \times n$ matrices with real entries forms a group under matrix multiplication.

The second of these groups is called the **general linear group of degree** $n$ (over the real numbers), and is denoted by $\mathrm{GL}(n)$. This name is used because the word 'linear' is associated with matrix algebra – known as *linear algebra* (it arises from systems of linear equations) – and the word 'general' distinguishes this group from the *special linear group of degree* $n$, which is defined later in this section.

Throughout this book we will work frequently with $\mathrm{GL}(2)$, the group of invertible $2 \times 2$ matrices with real entries under matrix multiplication, and with some of its subgroups. This section introduces you to some of these subgroups. We will assume throughout that by 'matrix' we mean a matrix with entries that are real numbers (rather than complex numbers, for example).

First, here is a reminder of some important properties of $2 \times 2$ matrices that we will need. You met these properties in Unit C1. Most of them generalise to properties of $n \times n$ matrices, but in Book E we will need them only for $2 \times 2$ matrices.

In the box below, and generally throughout this book, we write a product of two matrices in the form $\mathbf{AB}$, in the usual way, rather than making the binary operation explicit by writing $\mathbf{A} \times \mathbf{B}$.

### Properties of $2 \times 2$ matrices

1. The $2 \times 2$ **identity matrix**

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

has the property that

$$\mathbf{AI} = \mathbf{A} = \mathbf{IA}$$

for each $2 \times 2$ matrix $\mathbf{A}$.

2. If $\mathbf{A}$ is a $2 \times 2$ matrix, then there *may* exist a $2 \times 2$ matrix, denoted by $\mathbf{A}^{-1}$, such that

$$\mathbf{A}\mathbf{A}^{-1} = \mathbf{I} = \mathbf{A}^{-1}\mathbf{A}.$$

If such a matrix $\mathbf{A}^{-1}$ exists, then it is unique and is called the **inverse** of $\mathbf{A}$, and we say that $\mathbf{A}$ is **invertible**.

3. The **determinant** of $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is given by

$$\det \mathbf{A} = ad - bc.$$

A $2 \times 2$ matrix $\mathbf{A}$ is invertible if and only if $\det \mathbf{A} \neq 0$.

4. If $\mathbf{A} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is invertible, then

$$\mathbf{A}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

5. For all $2 \times 2$ matrices $\mathbf{A}$ and $\mathbf{B}$,

$$\det(\mathbf{AB}) = (\det \mathbf{A})(\det \mathbf{B}).$$

6. For all invertible $2 \times 2$ matrices $\mathbf{A}$ and $\mathbf{B}$,

$$(\mathbf{AB})^{-1} = \mathbf{B}^{-1}\mathbf{A}^{-1},$$

$$(\mathbf{A}^{-1})^{-1} = \mathbf{A},$$

$$\det \mathbf{A}^{-1} = \frac{1}{\det \mathbf{A}}.$$

## Exercise E18

Determine whether each of the following matrices is invertible, and write down its inverse if it exists.

(a) $\begin{pmatrix} 1 & 3 \\ 0 & 2 \end{pmatrix}$ (b) $\begin{pmatrix} 2 & -2 \\ 1 & -1 \end{pmatrix}$

Although you have already seen in Subsection 4.1 of Unit C1 that the set of invertible $2 \times 2$ matrices is a group under matrix multiplication, a proof of this fact is given below, to help familiarise you with this group. The proof given here is only for $2 \times 2$ matrices, rather than more generally for $n \times n$ matrices, as this is all we need here.

**Theorem E1**

The set of invertible $2 \times 2$ matrices is a group under matrix multiplication.

**Proof** Let $G$ be the set of invertible $2 \times 2$ matrices. We show that the four group axioms hold for $G$ under matrix multiplication.

**G1 Closure**

Let $\mathbf{A}$ and $\mathbf{B}$ be any elements of $G$. Then $\mathbf{AB}$ is a $2 \times 2$ matrix. Also, since $\mathbf{A}$ and $\mathbf{B}$ are invertible, $\det \mathbf{A} \neq 0$ and $\det \mathbf{B} \neq 0$, so

$$\det(\mathbf{AB}) = (\det \mathbf{A})(\det \mathbf{B}) \neq 0.$$

Hence $\mathbf{AB}$ is invertible. Therefore $\mathbf{AB} \in G$. So $G$ is closed under matrix multiplication.

**G2 Associativity**

Matrix multiplication is associative.

**G3 Identity**

The $2 \times 2$ identity matrix $\mathbf{I}$ is an invertible $2 \times 2$ matrix, so $\mathbf{I} \in G$ and we have

$$\mathbf{AI} = \mathbf{A} = \mathbf{IA}$$

for each $\mathbf{A} \in G$. Thus $\mathbf{I}$ is an identity element in $G$.

**G4 Inverses**

Let $\mathbf{A}$ be any element of $G$. Then $\mathbf{A}$ is invertible, so its inverse $\mathbf{A}^{-1}$ exists and is itself an invertible $2 \times 2$ matrix (with inverse $\mathbf{A}$). Hence $\mathbf{A}^{-1} \in G$ and we have

$$\mathbf{A}\mathbf{A}^{-1} = \mathbf{I} = \mathbf{A}^{-1}\mathbf{A}.$$

Thus each element $\mathbf{A} \in G$ has an inverse element $\mathbf{A}^{-1} \in G$.

Hence $(G, \times)$ satisfies the four group axioms and so is a group. ■

As mentioned earlier, the group in Theorem E1 is called the **general linear group of degree** 2 and is denoted by GL(2).

Now let us look at some subgroups of GL(2). The first worked exercise in this subsection shows that the set of all *lower triangular* matrices in GL(2) is a subgroup of GL(2). Recall that a **lower triangular** matrix is a matrix each of whose entries above the main diagonal is zero. So a $2 \times 2$ lower triangular matrix is a matrix of the form

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix},$$

where $a, c, d \in \mathbb{R}$.

## Worked Exercise E7

Show that the set $L$ of lower triangular matrices in GL(2) is a subgroup of GL(2).

### Solution

We show that the three subgroup properties hold for $L$.

**SG1 Closure**

Let $\mathbf{A}, \mathbf{B} \in L$.

We need to show that $\mathbf{AB} \in L$. We know that $\mathbf{AB} \in \mathrm{GL}(2)$ since $\mathbf{A}, \mathbf{B} \in \mathrm{GL}(2)$ and GL(2) is a group, so all we need to show is that $\mathbf{AB}$ is lower triangular.

Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ x & y \end{pmatrix},$$

for some $r, t, u, v, x, y \in \mathbb{R}$. Hence

$$\mathbf{AB} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix} \begin{pmatrix} v & 0 \\ x & y \end{pmatrix} = \begin{pmatrix} rv & 0 \\ tv + ux & uy \end{pmatrix}.$$

This is a lower triangular matrix, so $\mathbf{AB} \in L$.

Thus $L$ is closed under matrix multiplication.

**SG2 Identity**

The identity element $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ of GL(2) is lower triangular.

Hence $\mathbf{I} \in L$.

**SG3 Inverses**

Let $\mathbf{A} \in L$.

We need to show that $\mathbf{A}^{-1} \in L$. We know that $\mathbf{A}^{-1} \in \mathrm{GL}(2)$ since $\mathbf{A} \in \mathrm{GL}(2)$ and GL(2) is a group, so all we need to show is that $\mathbf{A}^{-1}$ is lower triangular.

Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ t & u \end{pmatrix},$$

for some $r, t, u \in \mathbb{R}$.

The inverse of $\mathbf{A}$ in GL(2) is

$$\mathbf{A}^{-1} = \frac{1}{ru}\begin{pmatrix} u & 0 \\ -t & r \end{pmatrix} = \begin{pmatrix} 1/r & 0 \\ -t/ru & 1/u \end{pmatrix}.$$

This is a lower triangular matrix, so $\mathbf{A}^{-1} \in L$. Thus $L$ contains the inverse of each of its elements.

Since the three subgroup properties hold, $L$ is a subgroup of GL(2).

The set $L$ in Worked Exercise E7, that is, the set of lower triangular matrices in GL(2), can be described without reference to GL(2) as the set of invertible $2 \times 2$ lower triangular matrices. We can specify it algebraically by using the fact that the $2 \times 2$ lower triangular matrix

$$\begin{pmatrix} a & 0 \\ c & d \end{pmatrix}$$

is invertible if and only if its determinant

$$ad - 0 \times c = ad$$

is non-zero. This gives

$$L = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

It can be shown in a similar way to the solution to Worked Exercise E7 that the set $U$ of all *upper triangular* matrices in GL(2) is a subgroup of GL(2). Remember that an **upper triangular** matrix is a matrix each of whose entries below the main diagonal is zero. The group $U$ can be specified in a similar way to the group $L$ as follows:

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

The next exercise is about the set $D$ of all *diagonal* matrices in GL(2). Remember that a **diagonal** matrix is a matrix each of whose entries not on the main diagonal is 0. So a $2 \times 2$ diagonal matrix is a matrix of the form

$$\begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix},$$

where $a, d \in \mathbb{R}$.

## Exercise E19

Show that the set $D$ of diagonal matrices in GL(2) is a subgroup of GL(2).

The next exercise introduces another subgroup of GL(2).

## Exercise E20

Show that the set $H$ of matrices in GL(2) with determinant 1 is a subgroup of GL(2).

The group in Exercise E20 is called the **special linear group of degree** 2 and is denoted by SL(2). (The proof in the solution to Exercise E20 can be generalised to show that for any positive integer $n$ the set of matrices in GL($n$) with determinant 1 is a subgroup of GL($n$); this group is known as the *special linear group of degree* $n$ (over the real numbers) and is denoted by SL($n$).)

The general linear group GL(2) and the four subgroups of GL(2) that you have met so far will be used frequently later in this book, and are summarised in the box below.

### Some standard matrix groups

The group GL(2), the group of all invertible $2 \times 2$ matrices under matrix multiplication, is given by

$$\mathrm{GL}(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R},\ ad - bc \neq 0 \right\}.$$

Its subgroups include the following.

- The group SL(2) of all $2 \times 2$ matrices with determinant 1:

$$\mathrm{SL}(2) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{R},\ ad - bc = 1 \right\}.$$

- The group $L$ of all invertible $2 \times 2$ lower triangular matrices:

$$L = \left\{ \begin{pmatrix} a & 0 \\ c & d \end{pmatrix} : a, c, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

- The group $U$ of all invertible $2 \times 2$ upper triangular matrices:

$$U = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} : a, b, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

- The group $D$ of all invertible $2 \times 2$ diagonal matrices:

$$D = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R},\ ad \neq 0 \right\}.$$

The group GL(2) has very many more subgroups than the four above.

The next worked exercise concerns a subgroup of GL(2) whose description is a little more complicated than those that you have met so far.

## Worked Exercise E8

Show that the set

$$Y = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$$

is a group under matrix multiplication.

### Solution

The set $Y$ is a *subset* of the group GL(2), because each matrix

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$$

in $Y$ has determinant

$$1 \times 1 - b \times 0 = 1$$

and is therefore invertible. Also, the binary operation specified for $Y$ is the same as the binary operation of GL(2).

Therefore, to show that $Y$ is a group, we can show that it is a subgroup of GL(2): we do not need to check the four group axioms from scratch.

We show that the three subgroup properties hold for $Y$.

**SG1 Closure**

Let $\mathbf{A}, \mathbf{B} \in Y$. Then

$$\mathbf{A} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

for some $m, n \in \mathbb{Z}$. So

$$\mathbf{AB} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & m+n \\ 0 & 1 \end{pmatrix}.$$

To check that $\mathbf{AB} \in Y$, we have to check that it is of the form specified before the colon in the definition of $Y$, namely

$$\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix},$$

and also that it satisfies the condition given after the colon, namely $b \in \mathbb{Z}$.

This matrix is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = m + n$. Also $m + n$ is an integer since both $m$ and $n$ are integers. So $\mathbf{AB} \in Y$. Thus $Y$ is closed under matrix multiplication.

**SG2 Identity**

The identity element

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of GL(2) is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = 0$. Thus $\mathbf{I} \in Y$.

**SG3 Inverses**

Let $\mathbf{A} \in Y$. Then

$$\mathbf{A} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix},$$

for some $n \in \mathbb{Z}$. The inverse of $\mathbf{A}$ in GL(2) is

$$\mathbf{A}^{-1} = \frac{1}{1}\begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}.$$

This matrix is of the form $\begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix}$ with $b = -n$. Also, $-n$ is an integer since $n$ is an integer. So $\mathbf{A}^{-1} \in Y$. Thus $Y$ contains the inverse of each of its elements.

Since the three subgroup properties hold, $Y$ is a subgroup of GL(2). Hence it is a group under matrix multiplication.

Notice that when subgroup property SG1 was checked in Worked Exercise E8, the two general elements $\mathbf{A}$ and $\mathbf{B}$ of the set

$$Y = \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} : b \in \mathbb{Z} \right\}$$

were taken to be

$$\mathbf{A} = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

So two new symbols, $m$ and $n$, were chosen to represent the two variables needed; the symbol $b$ from the definition of the set $Y$ was not used at all. It is sometimes convenient to choose completely new symbols in this way, to prevent possible confusion when we later compare an element that we have found (such as a product matrix $\mathbf{AB}$ or an inverse matrix $\mathbf{A}^{-1}$) to the general form of an element of a set. An alternative to choosing completely new symbols is to use subscripts: for example, here we could take

$$\mathbf{A} = \begin{pmatrix} 1 & b_1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} 1 & b_2 \\ 0 & 1 \end{pmatrix}.$$

The next worked exercise involves a subset of GL(2) that is *not* a subgroup.

## Worked Exercise E9

Show that the subset

$$W = \left\{ \begin{pmatrix} a & 1 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R},\ ad \neq 0 \right\}$$

of GL(2) is not a subgroup of GL(2).

### Solution

Subgroup property SG2 fails for $W$, because the identity element $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ of GL(2) is not in $W$, since its top right entry is not 1.

Here are some similar exercises for you to try.

## Exercise E21

Show that the following are groups under matrix multiplication, by showing that they are subgroups of GL(2).

(a) $M = \left\{ \begin{pmatrix} a & b \\ 0 & a \end{pmatrix} : a, b \in \mathbb{R},\ a \neq 0 \right\}$

(b) $P = \left\{ \begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix} : a \in \mathbb{R},\ a \neq 0 \right\}$

## Exercise E22

Show that the subset

$$X = \left\{ \begin{pmatrix} a & b \\ c & 1 \end{pmatrix} : a, b, c \in \mathbb{R},\ a - bc \neq 0 \right\}$$

of GL(2) is not a subgroup of GL(2).

The group GL(2) also has non-trivial *finite* subgroups. For example, you saw in Exercise E3 in Subsection 1.1 that the set of matrices $\{\mathbf{I}, \mathbf{R}, \mathbf{S}, \mathbf{T}\}$ is a group under matrix multiplication, where

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ \mathbf{R} = \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix},\ \mathbf{S} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},\ \mathbf{T} = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Each of these matrices is in GL(2), since each of them has a non-zero determinant.

# 3 Group structures

This section contains revision of four topics from Book B that relate to the structures of groups, namely the *order of a group element*, *cyclic subgroups*, *cyclic groups* and *isomorphic groups*.

## 3.1 Order of a group element

In this first subsection you will revise the idea of the *order* of a group element. This is a different concept from the order of a *group*, which as you have seen means the number of elements in the group.

First, here is a reminder about *multiplicative notation* and *additive notation*.

We use **multiplicative notation** for abstract groups (such as the general groups mentioned in theorems, proofs and general discussions about groups) and for groups whose binary operation is some kind of multiplication, or function composition. We call such groups **multiplicative** groups.

We use **additive notation** for groups whose binary operation is some kind of addition, and we call such groups **additive** groups.

The box below summarises the two types of notation.

### Multiplicative notation and additive notation for groups

| Feature | Multiplicative notation | Additive notation |
|---|---|---|
| Composite | $a \circ b$ or $a \times b$ or $ab$ (or similar) | $a + b$ (or similar) |
| Identity | $e$ or $1$ | $0$ |
| Inverse | $x^{-1}$ | $-x$ |
| Power/multiple | $x^n$ | $nx$ |

The last row of the table in the box above relates to the following conventions.

If we repeatedly compose an element $x$ of a *multiplicative* group with itself, then we call the resulting element a **power** of $x$, as follows.

### Definition

**Powers** of an element $x$ of a multiplicative group $(G, \circ)$ are defined as follows. Let $n$ be a positive integer. Then

$$x^0 = e, \quad \text{the identity element}$$

$$x^n = \underbrace{x \circ x \circ \cdots \circ x}_{n \text{ copies of } x}$$

$$x^{-n} = \underbrace{x^{-1} \circ x^{-1} \circ \cdots \circ x^{-1}}_{n \text{ copies of } x^{-1}}.$$

All powers of $x$ are elements of $G$, since $G$ is closed under $\circ$.

If we repeatedly compose an element $x$ of an *additive* group with itself, then we call the resulting element a **multiple** of $x$, as follows.

### Definition

**Multiples** of an element $x$ of an additive group $(G, +)$ are defined as follows. Let $n$ be a positive integer. Then

$$0x = e, \quad \text{the identity element}$$

$$nx = \underbrace{x + x + \cdots + x}_{n \text{ copies of } x}$$

$$-nx = \underbrace{(-x) + (-x) + \cdots + (-x)}_{n \text{ copies of } -x}.$$

All multiples of $x$ are elements of $G$, since $G$ is closed under $+$.

Most results and discussions in group theory are stated in multiplicative notation. To apply them to an additive group, you have to translate them into additive notation.

For example, the following boxes state the index laws for group elements and the versions obtained when they are translated into additive notation. You met these laws in Unit B2.

### Theorem B27 Index laws

Let $x$ be an element of a group $(G, \circ)$, and let $m$ and $n$ be integers. The following index laws hold.

(a) $x^m \circ x^n = x^{m+n}$

(b) $(x^m)^n = x^{mn}$

(c) $(x^n)^{-1} = x^{-n} = (x^{-1})^n$

### Theorem B28 Index laws (in additive notation)

Let $x$ be an element of a group $(G, +)$, and let $m$ and $n$ be integers. The following laws hold.

(a) $mx + nx = (m + n)x$

(b) $n(mx) = (nm)x$

(c) $-(nx) = (-n)x = n(-x)$

Usually group theory results and discussions will not be explicitly translated into additive notation for you, as that would complicate and lengthen the text. Occasionally the versions in additive notation are given for clarity, but most often you will have to do the translation yourself as needed.

### Exercise E23

Translate the following statements about an element $x$ of a multiplicative group $(G, \circ)$ into additive notation for an element $x$ of an additive group $(G, +)$.

(a) $x^3 \circ x = x^4$ (b) $x^5 \circ x^{-5} = e$ (c) $(x^4)^{-1} = (x^{-1})^4$

We can now define what is meant by the *order of a group element*.

### Definitions

Let $x$ be an element of a group $(G, \circ)$.

If there is a positive integer $n$ such that $x^n = e$, then the **order** of $x$ is the *smallest* positive integer $n$ such that $x^n = e$. We say that $x$ has **finite order**.

If there is no positive integer $n$ such that $x^n = e$, then $x$ has **infinite order**.

## Worked Exercise E10

Determine the order of each of the following group elements.

(a) $c$ in $S(\square)$ (shown in Figure 16) (b) 2 in $(\mathbb{R}^*, \times)$

### Solution

(a) In $S(\square)$ we have

$$c^1 = c,$$
$$c^2 = c \circ c = b,$$
$$c^3 = c^2 \circ c = b \circ c = a,$$
$$c^4 = c^3 \circ c = a \circ c = e.$$

We have shown that the *smallest* positive integer $n$ such that $c^n = e$ is 4.

Thus $c$ has order 4 in $S(\square)$.

(b) We have

$$2^1 = 2, \quad 2^2 = 4, \quad 2^3 = 8, \quad 2^4 = 16, \quad \ldots.$$

No matter how long we keep going we will not reach a positive integer $n$ such that $2^n$ is equal to the identity element 1 of $(\mathbb{R}^*, \times)$.

There is no positive integer $n$ such that $2^n = 1$, so 2 has infinite order in $(\mathbb{R}^*, \times)$.

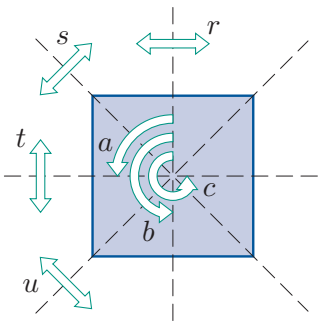



**Figure 16** $S(\square)$

You met the following results in Unit B2.

### Orders of elements in finite and infinite groups

- In every group, the identity element $e$ has order 1.
- If the group element $x$ is self-inverse and $x \neq e$, then $x$ has order 2.

**Theorem B29** Every element of a finite group has finite order.

**Theorem B30** A group element and its inverse either have the same finite order, or they both have infinite order.

## Exercise E24

Determine the order of each of the following group elements.

(a) In $S(\square)$: (i) $a$ (ii) $b$ (iii) $r$

(b) In $(U_9, \times_9)$: (i) 5 (ii) 2 (iii) 7

(c) In $(\mathbb{Z}_8, +_8)$: (i) 2 (ii) 3 (iii) 6

## Exercise E25

Find the order of each of the following elements of the group GL(2).

(a) $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (c) $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

You met the following important theorem in Unit B2. Part (a) of the theorem is illustrated in Figure 17.

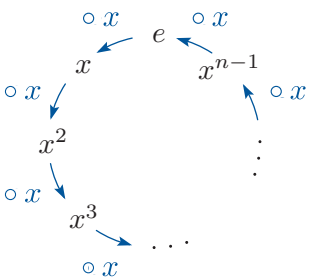



**Figure 17** The cycle of powers of an element $x$ of order $n$

### Theorem B31

Let $x$ be an element of a group $(G, \circ)$.

(a) If $x$ has finite order $n$, then the $n$ powers

$$e, x, x^2, \ldots, x^{n-1}$$

are distinct, and these elements repeat indefinitely every $n$ powers in the list of consecutive powers of $x$.

(b) If $x$ has infinite order, then all the powers of $x$ are distinct.

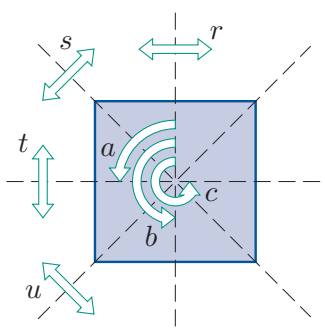



**Figure 18** $S(\square)$

For example, in $S(\square)$ (see Figure 18), the element $c$ has order 4, and the list of consecutive powers of $c$ in $S(\square)$ (including the zeroth power and the negative powers) is

$$\ldots,\ c^{-4}, c^{-3}, c^{-2}, c^{-1}, c^0,\ c^1,\ c^2,\ c^3,\ c^4,\ c^5,\ c^6,\ c^7,\ c^8,\ \ldots,$$

which evaluates to

$$\ldots,\ e,\quad c,\quad b,\quad a,\quad e,\quad c,\quad b,\quad a,\quad e,\quad c,\quad b,\quad a,\ \ldots.$$

So the powers $e, c, c^2, c^3$, that is, $e, c, b, a$, repeat indefinitely every 4 powers, as shown in Figure 19.

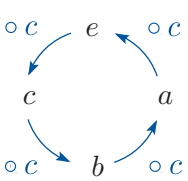



**Figure 19** The cycle of powers of the element $c$ in $S(\square)$

You met another important theorem about the orders of group elements in Unit B4.

### Corollary B69 to Lagrange's Theorem

Let $g$ be an element of a finite group $G$. Then the order of $g$ divides the order of $G$.

Finally in this subsection, let us look at how to find the order of an element of a symmetric group, that is, the order of a permutation. One method is to find its consecutive powers, as for any group element, but there is a much quicker method, as follows.

### Order of a permutation in cycle form

The order of a permutation in cycle form is the least common multiple of the lengths of its cycles.

For example, the permutation (1 3 4)(2 6)(5 9 7 8) in $S_9$ has cycles of lengths 3, 2 and 4, so its order is the least common multiple of 3, 2 and 4, which is 12.

### Exercise E26

State the orders of the following permutations in $S_9$.

(a) (2 3)(6 9 8) (b) (1 7 3 2 4) (c) (1 7)(3 6 4 5)

## 3.2 Cyclic subgroups

If $x$ is an element of a group $(G, \circ)$, then we denote the set of all powers of $x$ (including the zeroth power and all negative powers) by $\langle x \rangle$. That is,

$$\langle x \rangle = \{x^k : k \in \mathbb{Z}\}.$$

In the case of an element $x$ of an *additive* group $(G, +)$, the set $\langle x \rangle$ is the set of all multiples of $x$:

$$\langle x \rangle = \{kx : k \in \mathbb{Z}\}.$$

The theorem below was proved in Unit B2.

### Theorem B32

Let $x$ be an element of a group $(G, \circ)$. Then $(\langle x \rangle, \circ)$ is a subgroup of $(G, \circ)$.

The subgroup $(\langle x \rangle, \circ)$ in Theorem B32 is called the **cyclic subgroup of** $(G, \circ)$ **generated by** $x$. It may contain infinitely many elements, or, if the powers (or multiples) of $x$ are not all distinct, only finitely many elements.

For example, in $S(\square)$, whose non-identity elements are shown in Figure 20, the powers of the element $c$ are

$$\ldots, e, c, b, a, e, c, b, a, e, c, b, a, \ldots,$$

so

$$\langle c \rangle = \{e, a, b, c\}.$$

Similarly, in $(\mathbb{Z}_9, +_9)$ the multiples of the element 3 are

$$\ldots, 0, 3, 6, 0, 3, 6, 0, 3, 6, \ldots,$$

so

$$\langle 3 \rangle = \{0, 3, 6\}.$$

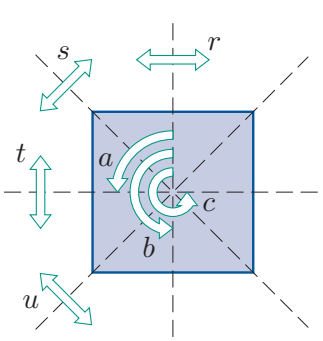



**Figure 20** $S(\square)$

In $(\mathbb{Z}, +)$ the multiples of the element 7 are

$$\ldots, -21, -14, -7, 0, 7, 14, 21, \ldots$$

(there is no repeating pattern), so

$$\langle 7 \rangle = \{\ldots, -21, -14, -7, 0, 7, 14, 21, \ldots\}.$$

These examples illustrate the following theorem.

### Theorem B33

Let $x$ be an element of a group $(G, \circ)$.

(a) If $x$ has finite order $n$, then the subgroup $\langle x \rangle$ has order $n$.

In multiplicative notation,

$$\langle x \rangle = \{e, x, x^2, \ldots, x^{n-1}\}.$$

In additive notation,

$$\langle x \rangle = \{0, x, 2x, \ldots, (n-1)x\}.$$

(b) If $x$ has infinite order, then the subgroup $\langle x \rangle$ has infinite order.

In multiplicative notation,

$$\langle x \rangle = \{\ldots, x^{-2}, x^{-1}, e, x, x^2, \ldots\}.$$

In additive notation,

$$\langle x \rangle = \{\ldots, -2x, -x, 0, x, 2x, \ldots\}.$$

Theorem B33 shows in particular that there is a close connection between the two meanings of the word *order* in group theory: the order of an element $x$ is equal to the order of the cyclic subgroup generated by $x$. For example, in $S(\square)$ the element $c$ has order 4 and the subgroup

$$\langle c \rangle = \{e, c, c^2, c^3\} = \{e, a, b, c\}$$

has order 4.

### Exercise E27

By using the solution to Exercise E24, determine the cyclic subgroup generated by each of the following group elements.

(a) In $S(\square)$: (i) $a$ (ii) $b$ (iii) $r$

(b) In $(U_9, \times_9)$: (i) 5 (ii) 2 (iii) 7

(c) In $(\mathbb{Z}_8, +_8)$: (i) 2 (ii) 3 (iii) 6

Two different elements of a group can generate the same cyclic subgroup. For example, in $S(\square)$ the elements $a$ and $c$ do this:

$$\langle a\rangle = \{e, a, a^2, a^3\} = \{e, a, b, c\},$$

$$\langle c\rangle = \{e, c, c^2, c^3\} = \{e, c, b, a\} = \{e, a, b, c\} = \langle a\rangle.$$

You saw other examples of this in Exercise E27.

The following simple results about cyclic subgroups were proved in Subsection 3.1 of Unit B2.

### Some special cyclic subgroups

Let $(G, \circ)$ be a group with identity element $e$, and let $x \in G$.

- $\langle e\rangle = \{e\}$.
- If $x$ is self-inverse and $x \neq e$, then $\langle x\rangle = \{e, x\}$.
- $\langle x^{-1}\rangle = \langle x\rangle$ (or, in additive notation, $\langle -x\rangle = \langle x\rangle$).

### Exercise E28

For each of the following groups, determine the cyclic subgroup generated by each of its elements, and list the distinct cyclic subgroups of the group, stating how many there are.

(a) $S(\square)$ (b) $(\mathbb{Z}_9, +_9)$ (c) $(\mathbb{Z}_7^*, \times_7)$ (d) $S_3$

## 3.3 Cyclic groups

We make the following definitions.

### Definitions

A group $G$ is **cyclic** if it contains an element $x$ such that $G = \langle x\rangle$. Such an element $x$ is called a **generator** of the group.

A group that is not cyclic is called **non-cyclic**.

For example, in $(\mathbb{Z}_9, +_9)$,

$$\langle 1\rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = \mathbb{Z}_9,$$

so $(\mathbb{Z}_9, +_9)$ is a cyclic group, and 1 is a generator of this group. In fact, the elements 2, 4, 5, 7 and 8 are also generators of $(\mathbb{Z}_9, +_9)$, as you can see from the solution to Exercise E28(b).

The theorem below follows immediately from the fact that a group element of order $n$ generates a cyclic subgroup of order $n$ (Theorem B33(a)).

### Theorem B34

A finite group of order $n$ is cyclic if and only if it contains an element of order $n$.

## Exercise E29

Determine which of the following groups are cyclic. State all the generators of each cyclic group.

(a) $S(\square)$ (b) $S^+(\square)$ (c) $(\mathbb{Z}_5, +_5)$ (d) $(U_8, \times_8)$

In Unit B2 you met the following theorems about cyclic groups.

**Theorem B35** Every cyclic group is abelian.

**Theorem B36** Every subgroup of a cyclic group is cyclic.

You also studied the standard cyclic groups $(\mathbb{Z}_n, +_n)$, where $n \geq 2$, in detail, and met the following theorems.

### The group $(\mathbb{Z}_n, +_n)$ $(n \geq 2)$

**Theorem B37** The group $(\mathbb{Z}_n, +_n)$ is cyclic, and one of its generators is 1.

**Theorem B38** If $m$ is a non-zero element of $(\mathbb{Z}_n, +_n)$, then $m$ has order $n/d$, where $d$ is the highest common factor of $m$ and $n$.

**Corollary B40** The element $m$ of $(\mathbb{Z}_n, +_n)$ is a generator of $(\mathbb{Z}_n, +_n)$ if and only if $m$ is coprime to $n$.

## Exercise E30

(a) Find the order of each element of the group $(\mathbb{Z}_{14}, +_{14})$.

(b) State the generators of the group $(\mathbb{Z}_{14}, +_{14})$.

The following theorem describes all the subgroups of each group $(\mathbb{Z}_n, +_n)$, where $n \geq 2$.

**Theorem B41 Subgroups of $(\mathbb{Z}_n, +_n)$**

The group $(\mathbb{Z}_n, +_n)$ has exactly one cyclic subgroup of order $q$ for each positive factor $q$ of $n$, and no other subgroups.

- The subgroup of order 1 is generated by 0.
- For each other factor $q$ of $n$, the subgroup of order $q$ is generated by $d$, where $qd = n$.

**Exercise E31**

Write down all the distinct cyclic subgroups of the group $(\mathbb{Z}_{16}, +_{16})$, listing the elements of each subgroup and giving each subgroup once only.

## 3.4 Isomorphic groups

In this subsection we will revise what it means for two groups to be *isomorphic*.

Consider the five groups of order 4 whose group tables are given below.

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

$(S^+(\square), \circ)$

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

$(\mathbb{Z}_4, +_4)$

| $\times_5$ | 1 | 2 | 3 | 4 |
|---|---|---|---|---|
| 1 | 1 | 2 | 3 | 4 |
| 2 | 2 | 4 | 1 | 3 |
| 3 | 3 | 1 | 4 | 2 |
| 4 | 4 | 3 | 2 | 1 |

$(\mathbb{Z}_5^*, \times_5)$

| $\circ$ | $e$ | $a$ | $r$ | $s$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $r$ | $s$ |
| $a$ | $a$ | $e$ | $s$ | $r$ |
| $r$ | $r$ | $s$ | $e$ | $a$ | 
| $s$ | $s$ | $r$ | $a$ | $e$ |

$(S(\square), \circ)$

| $\times_8$ | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

$(U_8, \times_8)$

In one sense, all these groups are different, because their sets and binary operations are different. Superficially, they have a 'sameness' in that they all have four elements. The idea of isomorphism is much stronger than this: two groups are **isomorphic** if they have identical structures – that is, if one of the groups can be obtained from the other by 'renaming' the elements and the binary operation.

For finite groups we can define this concept more rigorously as follows: two finite groups are *isomorphic* if there is a one-to-one and onto mapping from one group to the other group that transforms a group table for the first group into a group table for the second group. Such a mapping is called an **isomorphism**. (The isomorphism 'renames' the elements.) Remember that 'mapping' is just another word for 'function'.

For example, consider the first two of the five groups above, $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$, whose group tables are repeated below.

| $\circ$ | $e$ | $a$ | $b$ | $c$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ |
| $a$ | $a$ | $b$ | $c$ | $e$ |
| $b$ | $b$ | $c$ | $e$ | $a$ |
| $c$ | $c$ | $e$ | $a$ | $b$ |

$(S^+(\square), \circ)$

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

$(\mathbb{Z}_4, +_4)$

If we take the group table of $(S^+(\square), \circ)$ and replace each element in it with an element of $(\mathbb{Z}_4, +_4)$ according to the 'renaming' mapping

$$\begin{aligned} \phi : S^+(\square) &\longrightarrow \mathbb{Z}_4 \\ e &\longmapsto 0 \\ a &\longmapsto 1 \\ b &\longmapsto 2 \\ c &\longmapsto 3 \end{aligned}$$

(and also replace the symbol $\circ$ in the table with the symbol $+_4$), then we obtain the group table of $(\mathbb{Z}_4, +_4)$, as you can check. So these two groups are isomorphic, and the mapping $\phi$ is an isomorphism.

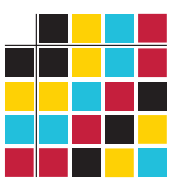


**Figure 21** The pattern of the group tables of $(S^+(\square), \circ)$ and $(\mathbb{Z}_4, +_4)$

The reason why the group table of $(\mathbb{Z}_4, +_4)$ can be obtained from the group table of $(S^+(\square), \circ)$ by 'renaming' the elements is that the two group tables have exactly the same pattern. They both have the pattern of bottom left to top right diagonal stripes shown in Figure 21.

Now consider the third of the five groups above, $(\mathbb{Z}_5^*, \times_5)$. At first sight it looks as if it has a structure different from that of the first two groups, because its group table does not have the pattern of diagonal stripes in Figure 21. However, if we swap the elements 3 and 4 in the borders of the group table of $(\mathbb{Z}_5^*, \times_5)$, and rearrange the entries in the body of the table accordingly so that the table is still a correct group table for $(\mathbb{Z}_5^*, \times_5)$, then we obtain the following table:

| $\times_5$ | 1 | 2 | 4 | 3 |
|---|---|---|---|---|
| 1 | 1 | 2 | 4 | 3 |
| 2 | 2 | 4 | 3 | 1 |
| 4 | 4 | 3 | 1 | 2 |
| 3 | 3 | 1 | 2 | 4 |

This group table for $(\mathbb{Z}_5^*, \times_5)$ does have the pattern of diagonal stripes in Figure 21, so the group $(\mathbb{Z}_5^*, \times_5)$ *is* isomorphic to the first two groups. The following mapping, obtained by matching up the elements in the borders of the group table for $(S^+(\square), \circ)$ and the rearranged group table for $(\mathbb{Z}_5^*, \times_5)$, is an isomorphism:

$$\begin{aligned} \phi : S^+(\square) &\longrightarrow \mathbb{Z}_5^* \\ e &\longmapsto 1 \\ a &\longmapsto 2 \\ b &\longmapsto 4 \\ c &\longmapsto 3. \end{aligned}$$

Now consider the final two of the five groups above, $(S(\square), \circ)$ and $(U_8, \times_8)$, whose group tables are repeated below.

| $\circ$ | $e$ | $a$ | $r$ | $s$ |
|---|---|---|---|---|
| $e$ | $e$ | $a$ | $r$ | $s$ |
| $a$ | $a$ | $e$ | $s$ | $r$ |
| $r$ | $r$ | $s$ | $e$ | $a$ |
| $s$ | $s$ | $r$ | $a$ | $e$ |

$(S(\square), \circ)$

| $\times_8$ | 1 | 3 | 5 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 5 | 7 |
| 3 | 3 | 1 | 7 | 5 |
| 5 | 5 | 7 | 1 | 3 |
| 7 | 7 | 5 | 3 | 1 |

$(U_8, \times_8)$

**Figure 22** The pattern of the group tables of $(S(\square), \circ)$ and $(U_8, \times_8)$

These group tables have the same pattern as each other, namely the pattern shown in Figure 22, so these two groups are certainly isomorphic to each other.

To determine whether they are also isomorphic to the first three groups, we need to ascertain whether it is possible to rearrange the elements in the borders of their group tables to obtain group tables that have the diagonal stripes pattern in Figure 21. A little thought shows that this is *not* possible: in each of these two groups every element is self-inverse, so no matter how we rearrange the borders of their group tables, the four positions on the main diagonal will contain four occurrences of the identity element, whereas the diagonal stripes pattern has two different elements on the main diagonal. So the groups $(S(\square), \circ)$ and $(U_8, \times_8)$ are *not* isomorphic to the groups $(S^+(\square), \circ)$, $(\mathbb{Z}_4, +_4)$ and $(\mathbb{Z}_5^*, \times_5)$.

## Exercise E32

(a) List the elements of the group $(U_{10}, \times_{10})$.

(b) Construct a group table for this group.

(c) Show that $(U_{10}, \times_{10})$ is isomorphic to one of $(\mathbb{Z}_4, +_4)$ or $(S(\square), \circ)$ by finding an isomorphism from $(U_{10}, \times_{10})$ to one of these two groups.

You saw above that the condition for a one-to-one and onto mapping $\phi$ from a finite group $(G, \circ)$ to a finite group $(H, *)$ to be an isomorphism is that it must transform the group table of $(G, \circ)$ into a group table for $(H, *)$. This condition can be expressed algebraically as follows.

Consider any elements $x$ and $y$ of $G$, and their composite $x \circ y$ in the group table for $(G, \circ)$, as illustrated on the left below. In the table transformed by using the mapping $\phi$, these three elements are replaced by $\phi(x)$, $\phi(y)$ and $\phi(x \circ y)$, as illustrated on the right.

| $\circ$ | $\cdots$ | $y$ | $\cdots$ |
|---|---|---|---|
| $\vdots$ | | $\vdots$ | |
| $x$ | $\cdots$ | $x \circ y$ | $\cdots$ |
| $\vdots$ | | $\vdots$ | |

$(G, \circ)$

$\longrightarrow$

| $*$ | $\cdots$ | $\phi(y)$ | $\cdots$ |
|---|---|---|---|
| $\vdots$ | | $\vdots$ | |
| $\phi(x)$ | $\cdots$ | $\phi(x \circ y)$ | $\cdots$ |
| $\vdots$ | | $\vdots$ | |

$(H, *)$

If the table obtained is to be a correct group table for $(H, *)$, then the entry in the cell with row label $\phi(x)$ and column label $\phi(y)$ must be equal to $\phi(x) * \phi(y)$, so we must have

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

This applies to all elements $x$ and $y$ of $G$, so the condition for $\phi$ to be an isomorphism can be expressed algebraically as

$$\phi(x \circ y) = \phi(x) * \phi(y) \quad \text{for all } x, y \in G.$$

Thus we can define an isomorphism from a finite group $(G, \circ)$ to a finite group $(H, *)$ to be a one-to-one and onto mapping $\phi : (G, \circ) \longrightarrow (H, *)$ that satisfies the condition above. This also applies to *infinite* groups; the only difference is that we cannot write down group tables for such groups. So we have the following definitions.

### Definitions

Two groups $(G, \circ)$ and $(H, *)$ are **isomorphic** if there exists a mapping $\phi : G \longrightarrow H$ with the following properties.

(a) $\phi$ is one-to-one and onto.

(b) For all $x, y \in G$,

$$\phi(x \circ y) = \phi(x) * \phi(y).$$

Such a mapping $\phi$ is called an **isomorphism**.

We write $(G, \circ) \cong (H, *)$ to assert that the groups $(G, \circ)$ and $(H, *)$ are isomorphic.

## Exercise E33

The cyclic subgroup of the infinite additive group $(\mathbb{Z}, +)$ generated by the integer 3 is

$$\langle 3 \rangle = \{\ldots, -9, -6, -3, 0, 3, 6, 9, \ldots\},$$

and we denote this group by $3\mathbb{Z}$. Show that $(\mathbb{Z}, +) \cong (3\mathbb{Z}, +)$ by showing that the mapping

$$\begin{aligned} \phi : \mathbb{Z} &\longrightarrow 3\mathbb{Z} \\ n &\longmapsto 3n \end{aligned}$$

is an isomorphism.

The collection of all groups can be split (*partitioned*) into disjoint classes, which we call **isomorphism classes**, such that two groups belong to the same isomorphism class if they are isomorphic, and belong to different isomorphism classes otherwise.

Within each isomorphism class all the groups have the same order, since two groups cannot be isomorphic if they do not have the same order. However, two groups of the same order may not be isomorphic, so there may be more than one isomorphism class for groups of a particular order.

Earlier in this subsection you saw two different structures for groups of order 4. It was proved in Subsection 2.3 of Unit B4 that these two structures are the only possible structures for groups of order 4, so there are exactly two isomorphism classes for groups of order 4.

In fact you met all the isomorphism classes for groups of orders 1 to 8 in Section 2 of Unit B4. They are summarised in the table below. There is a row for each different isomorphism class, so the table shows that for each of the orders 1, 2, 3, 5 and 7 there is just one isomorphism class, whereas for each of the orders 4 and 6 there are two isomorphism classes, and for order 8 there are five isomorphism classes.

For each isomorphism class, the table gives one or two standard groups in the class. Where there is more than one isomorphism class for groups of a particular order, the table gives some distinguishing features of groups in the different classes. For example the table shows that if a group of order 6 is abelian (or contains an element of order 6), then it is isomorphic to the group $C_6$ (and to the group $\mathbb{Z}_6$).

Recall that the notation $C_n$, where $n$ is a positive integer, denotes a standard, abstract cyclic group of order $n$. The notation $V$ denotes the *Klein four-group*, which is a standard, abstract group isomorphic to $S(\square)$, the symmetry group of a rectangle. The notation $Q_8$ denotes the *quaternion group*, a group of order 8 that contains an identity element, one element of order 2 and six elements of order 4; its group table was given in Subsection 2.5 of Unit B4. The group $S(\text{cuboid})$ is the symmetry group of a cuboid with no square faces.

## Isomorphism classes for groups of orders 1 to 8

| Order | Standard group(s) | Distinguishing features (given the order of the group) |
|---|---|---|
| 1 | $C_1$ | |
| 2 | $C_2$, $\mathbb{Z}_2$ | |
| 3 | $C_3$, $\mathbb{Z}_3$ | |
| 4 | $C_4$, $\mathbb{Z}_4$ | Exactly 2 self-inverse elements.<br>An element of order 4. |
| | $V$, $S(\square)$ | All elements self-inverse. |
| 5 | $C_5$, $\mathbb{Z}_5$ | |
| 6 | $C_6$, $\mathbb{Z}_6$ | Abelian.<br>An element of order 6. |
| | $S(\triangle)$ | Non-abelian. |
| 7 | $C_7$, $\mathbb{Z}_7$ | |
| 8 | $C_8$, $\mathbb{Z}_8$ | Abelian with exactly 2 self-inverse elements.<br>An element of order 8. |
| | $S(\text{cuboid})$ | Abelian with all elements self-inverse. |
| | $U_{15}$ | Abelian with exactly 4 self-inverse elements. |
| | $S(\square)$ | Non-abelian with exactly 6 self-inverse elements. |
| | $Q_8$ | Non-abelian with exactly 2 self-inverse elements. |

*Where two sets of distinguishing features are given on separate lines in the same row of the table,* either *distinguishes the isomorphism class.*

Notice that the table does not state the binary operation of the standard groups. You are familiar with a symmetry group $(S(F), \circ)$ being denoted by just $S(F)$. In the same way, we will often use the following abbreviated notation throughout the rest of this book.

- The group $\mathbb{Z}_n$ means the group $(\mathbb{Z}_n, +_n)$.
- The group $U_n$ means the group $(U_n, \times_n)$.
- The group $\mathbb{Z}_p^*$ means the group $(\mathbb{Z}_p^*, \times_p)$ (where $p$ is prime).

These assumptions are natural: $\mathbb{Z}_n$ is a group under $+_n$ but not under $\times_n$, $U_n$ is a group under $\times_n$ but not under $+_n$, and (provided $p$ is prime) $\mathbb{Z}_p^*$ is a group under $\times_p$ but not under $+_p$.

## Exercise E34

State a standard group that is isomorphic to the group $(G, \times)$ of matrices whose group table you were asked to find in Exercise E3 in Subsection 1.1, justifying your answer.

## Exercise E35

Write down the elements of the group $U_{18}$. Without constructing a group table for this group, identify a standard group from the table of isomorphism classes above that is isomorphic to this group, justifying your answer.

The table of isomorphism classes in the box above indicates that there is only one isomorphism class for each of the orders 2, 3, 5 and 7. In fact there is only one isomorphism class for any prime order. This follows from the corollary below.

### Corollary B71 to Lagrange's Theorem

If $G$ is a group of prime order $p$, then $G$ is isomorphic to the cyclic group $(\mathbb{Z}_p, +_p)$.

You will revise isomorphisms further in Unit E3 *Homomorphisms*.

You have now finished the revision of Book B in this unit. In the rest of the unit you will be studying new material.

# 4 Cosets

In this section you will see how we can use a subgroup of a group to split the group in a natural way into disjoint subsets, one of which is the subgroup itself. You have already seen some examples of this. For instance, the group $S(\square)$ can be split into its subgroup of direct symmetries and its subset of indirect symmetries, as follows:

$$S(\square) = \{e, a, b, c\} \cup \{r, s, t, u\}.$$

Another example is that the group $\mathbb{Z}_{12}$ (that is, $(\mathbb{Z}_{12}, +_{12})$) can be split into its subgroup $\langle 4 \rangle = \{0, 4, 8\}$ and three other subsets obtained by 'shifting' this subgroup, that is, by adding (modulo 12) the same element of $\mathbb{Z}_{12}$ to each element of the subgroup:

$$\mathbb{Z}_{12} = \{0, 4, 8\} \cup \{1, 5, 9\} \cup \{2, 6, 10\} \cup \{3, 7, 11\}.$$

The second subset here is obtained by adding 1 to each element of the subgroup, the third subset by adding 2 and the fourth subset by adding 3.

In each of these two examples, the subsets are *cosets*, which you will learn about in this section.

Cosets are of fundamental importance in group theory. They are of two types: *left cosets* and *right cosets*. In the first subsection we will look at left cosets. Right cosets are similar and are dealt with in the second subsection.

Note that although so far in this unit we have usually denoted an abstract group by $(G, \circ)$, and a composite of two elements $x$ and $y$ of $G$ by $x \circ y$, for the remainder of the unit and in the rest of Book E we will often adopt the following useful convention, which you met in Unit B4.

### Convention

In discussions about abstract groups, we use the following notation and terminology where it will not cause confusion.

- We denote an abstract group simply by a single symbol such as $G$, without specifying a symbol for its binary operation.
- We denote a composite of two elements $x$ and $y$ of $G$ simply by $xy$.

*Warning*: Unless the group is abelian, the composites $xy$ and $yx$ are not necessarily equal.

We refer to multiplicative notation that uses this convention as *concise multiplicative notation*.

## 4.1 Left cosets

We begin with the definition of a *left coset*.

### Definition

Let $H$ be a subgroup of a group $G$, and let $g$ be an element of $G$. The **left coset** $gH$ of $H$ is given by

$$gH = \{gh : h \in H\}.$$

It is the subset of $G$ obtained by composing each element of $H$ with $g$ on the left.

This definition is expressed in the concise multiplicative notation described in the convention above, so you may need to translate it when you want to apply it to a particular group. For example, consider the subgroup $H = \langle r \rangle = \{e, r\}$ of the group $S(\square)$, and the element $a$ of $S(\square)$. The left coset $aH$ of $H$ in $S(\square)$ is

$$aH = a\{e, r\} = \{a \circ e, a \circ r\} = \{a, s\}.$$

Notice that, for brevity, we usually denote a left coset by notation of the form $gH$, not $g \circ H$, even if we are using the symbol $\circ$ to denote the binary operation.

The word 'left' in 'left coset' refers to the fact that to obtain the left coset $gH$ we compose each element of $H$ with $g$ on the left. *Right cosets* are obtained in a similar way but by composing on the right; you will study them in the next subsection.

You can think of a coset (either left or right) of a subgroup as being obtained by 'shifting' the subgroup, in the sense that to obtain the left coset $gH$, for example, we 'shift' every element of the subgroup $H$ in the same way, by composing it with the group element $g$ on the left. This is illustrated in Figure 23.

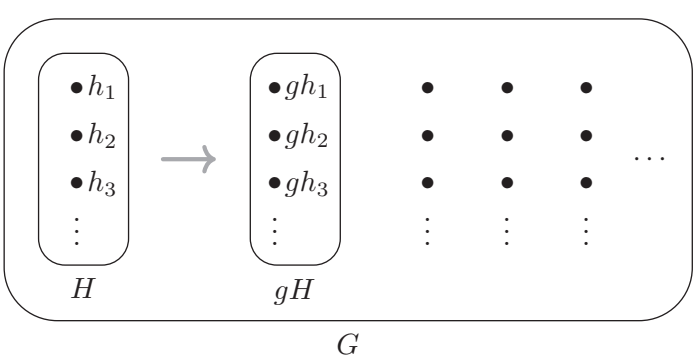



**Figure 23** A left coset of a subgroup $H$ in a group $G$ is a 'shift' of $H$

In the next worked exercise we find *all* the left cosets of the subgroup $H = \{e, r\}$ of the group $S(\square)$, by calculating the left coset $gH$ for each element $g$ in $S(\square)$ in turn.

**Table 5** $S(\square)$

| $\circ$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
| $a$ | $a$ | $b$ | $c$ | $e$ | $s$ | $t$ | $u$ | $r$ |
| $b$ | $b$ | $c$ | $e$ | $a$ | $t$ | $u$ | $r$ | $s$ |
| $c$ | $c$ | $e$ | $a$ | $b$ | $u$ | $r$ | $s$ | $t$ |
| $r$ | $r$ | $u$ | $t$ | $s$ | $e$ | $c$ | $b$ | $a$ |
| $s$ | $s$ | $r$ | $u$ | $t$ | $a$ | $e$ | $c$ | $b$ |
| $t$ | $t$ | $s$ | $r$ | $u$ | $b$ | $a$ | $e$ | $c$ |
| $u$ | $u$ | $t$ | $s$ | $r$ | $c$ | $b$ | $a$ | $e$ |

## Worked Exercise E11

Find all the left cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$. (The group table of $S(\square)$ is given as Table 5.)

### Solution

For each $g \in S(\square)$, we calculate the left coset $gH$.

$$
\begin{aligned}
eH &= e\{e,r\} = \{e\circ e, e\circ r\} = \{e,r\},\\
aH &= a\{e,r\} = \{a\circ e,\ a\circ r\} = \{a,s\},\\
bH &= b\{e,r\} = \{b\circ e,\ b\circ r\} = \{b,t\},\\
cH &= c\{e,r\} = \{c\circ e,\ c\circ r\} = \{c,u\},\\
rH &= r\{e,r\} = \{r\circ e,\ r\circ r\} = \{r,e\},\\
sH &= s\{e,r\} = \{s\circ e,\ s\circ r\} = \{s,a\},\\
tH &= t\{e,r\} = \{t\circ e,\ t\circ r\} = \{t,b\},\\
uH &= u\{e,r\} = \{u\circ e,\ u\circ r\} = \{u,c\}.
\end{aligned}
$$

Notice from Worked Exercise E11 that a left coset of a subgroup is not necessarily a subgroup itself.

Notice also that some of the left cosets found in Worked Exercise E11 turn out to be the same set. For example, both $eH$ and $rH$ are the set $\{e, r\}$. In fact there are only four *distinct* left cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$, because

$$
\begin{aligned}
eH &= rH = \{e,r\},\\
aH &= sH = \{a,s\},\\
bH &= tH = \{b,t\},\\
cH &= uH = \{c,u\}.
\end{aligned}
$$

So the distinct left cosets of $H = \{e, r\}$ in $S(\square)$ are

$$\{e,r\}, \quad \{a,s\}, \quad \{b,t\}, \quad \{c,u\}.$$

**Table 6** $S(\triangle)$

| $\circ$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
| $a$ | $a$ | $b$ | $e$ | $t$ | $r$ | $s$ |
| $b$ | $b$ | $e$ | $a$ | $s$ | $t$ | $r$ |
| $r$ | $r$ | $s$ | $t$ | $e$ | $a$ | $b$ |
| $s$ | $s$ | $t$ | $r$ | $b$ | $e$ | $a$ |
| $t$ | $t$ | $r$ | $s$ | $a$ | $b$ | $e$ |

## Exercise E36

(a) Find all the left cosets of the subgroup $H = \{e, s\}$ in the group $S(\triangle)$. (The group table of $S(\triangle)$ is given as Table 6.)

(b) List the distinct left cosets of $H = \{e, s\}$ in $S(\triangle)$.

## Exercise E37

(a) Show that $H = \{1, 2, 4\}$ is a subgroup of the group $\mathbb{Z}_7^*$. (Remember that we use $\mathbb{Z}_7^*$ to denote the group $(\mathbb{Z}_7^*, \times_7)$.)

(b) Find all the left cosets of $H$ in $\mathbb{Z}_7^*$.

(c) List the distinct left cosets of $H$ in $\mathbb{Z}_7^*$.

You saw just after Worked Exercise E11 that the distinct left cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$ are

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\}.$$

Notice that these sets form a *partition* of the group $S(\square)$, as illustrated in Figure 24. Remember that a **partition** of a set is a family of subsets of the set such that every element of the set belongs to one of the subsets, and each pair of the subsets are **disjoint** – that is, they have no elements in common. In other words, each element of the set belongs to *exactly one* of the subsets in the partition.

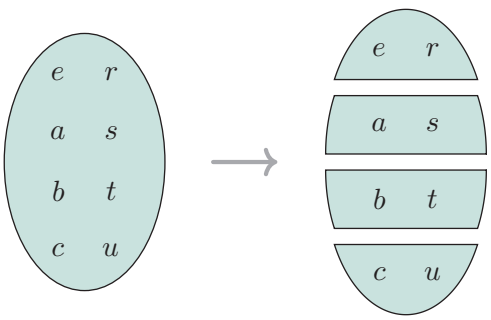



**Figure 24** The group $S(\square)$ partitioned into the left cosets of the subgroup $\{e, r\}$

Similarly, in each of Exercises E36 and E37 you should have found that the distinct left cosets of the subgroup form a partition of the group, as illustrated in Figure 25.

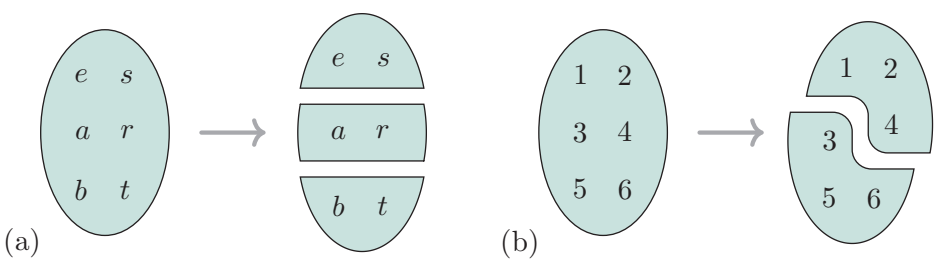



**Figure 25** Groups partitioned into left cosets of a subgroup: (a) $S(\triangle)$ with subgroup $\{e, s\}$ (b) $\mathbb{Z}_7^*$ with subgroup $\{1, 2, 4\}$

In fact, this always happens, as stated in the next theorem.

### Theorem E2

Let $H$ be a subgroup of a group $G$. Then the distinct left cosets of $H$ in $G$ form a partition of $G$.

To prove this theorem we use the properties of equivalence relations, which you met in Unit A3 *Mathematical language and proof*. Remember that $\sim$ is a *relation* on a set $X$ if, whenever $x, y \in X$, the statement $x \sim y$ is either true or false, and an *equivalence relation* is a relation with the properties in the definition below.

### Definition

A relation $\sim$ on a set $X$ is an **equivalence relation** if it has the following three properties.

**E1 Reflexivity** For all $x$ in $X$,

$$x \sim x.$$

**E2 Symmetry** For all $x, y$ in $X$,

$$\text{if } x \sim y, \text{ then } y \sim x.$$

**E3 Transitivity** For all $x, y, z$ in $X$,

$$\text{if } x \sim y \text{ and } y \sim z, \text{ then } x \sim z.$$

As you saw in Unit A3, if $\sim$ is an equivalence relation on a set $X$ and $x \in X$, then we call the set $\{y \in X : x \sim y\}$ the **equivalence class** of $x$ and denote it by $[\![x]\!]$. The key property of equivalence classes that we need is the following result from Unit A3.

### Theorem A16

The equivalence classes of an equivalence relation on a set $X$ form a partition of the set $X$.

We now apply these ideas to prove Theorem E2, which is repeated below. The overall method of the proof is that we define a particular relation on the set $G$, prove that it is an equivalence relation, and prove that its equivalence classes are the left cosets of $H$ in $G$. It then follows from Theorem A16 that these left cosets form a partition of $G$.

### Theorem E2

Let $H$ be a subgroup of a group $G$. Then the distinct left cosets of $H$ in $G$ form a partition of $G$.

**Proof** Let $\sim$ be the relation defined on $G$ by

$$x \sim y \quad \text{if } x \in yH.$$

We show that $\sim$ is an equivalence relation.

**E1 Reflexive property**

Let $x \in G$. We have to show that $x \sim x$, that is, $x \in xH$. This is true, because

$$x = xe$$

and $e \in H$, since $H$ is a subgroup. Hence $x \sim x$. Thus $\sim$ is reflexive.

**E2 Symmetric property**

Let $x, y \in G$, and suppose that $x \sim y$, that is, $x \in yH$. We have to show that $y \sim x$, that is, $y \in xH$. Since $x \in yH$, we have

$$x = yh$$

for some $h \in H$. Composing both sides of this equation with $h^{-1}$ on the right gives

$$xh^{-1} = yhh^{-1},$$

that is,

$$xh^{-1} = y.$$

Now $h^{-1} \in H$, since $H$ is a subgroup, so this shows that $y \in xH$, that is, $y \sim x$. Thus $\sim$ is symmetric.

**E3 Transitive property**

Let $x, y, z \in G$, and suppose that $x \sim y$ and $y \sim z$, that is, $x \in yH$ and $y \in zH$. We have to show that $x \sim z$, that is, $x \in zH$. Since $x \in yH$ and $y \in zH$, we have

$$x = yh_1 \quad \text{and} \quad y = zh_2$$

for some $h_1, h_2 \in H$. Using the second equation above to substitute for $y$ in the first equation gives

$$x = zh_2h_1.$$

Now $h_2h_1 \in H$, since $H$ is a subgroup, so this shows that $x \in zH$, that is, $x \sim z$. Thus $\sim$ is transitive.

Hence $\sim$ is an equivalence relation.

Each element $x$ in $G$ has equivalence class

$$\begin{aligned}[\![x]\!] &= \{y \in G : y \sim x\} \\ &= \{y \in G : y \in xH\} \\ &= xH.\end{aligned}$$

Thus the equivalence classes of $\sim$ are the left cosets of $H$ in $G$. It follows from Theorem A16 that the left cosets of $H$ in $G$ form a partition of $G$, as required. ■

Some simple but important properties of left cosets are given in the proposition below.

### Proposition E3 Properties of left cosets

Let $H$ be a subgroup of a group $G$.

(a) The element $g$ lies in the left coset $gH$, for each $g \in G$.

(b) One of the left cosets of $H$ in $G$ is $H$ itself.

(c) Any two left cosets $g_1H$ and $g_2H$ are either the same set or are disjoint.

(d) If $H$ is finite, then each left coset $gH$ has the same number of elements as $H$.

To illustrate these properties, consider again the left cosets of the subgroup $H = \{e, r\}$ of $S(\square)$, found in Worked Exercise E11:

$$eH = rH = \{e, r\},$$
$$aH = sH = \{a, s\},$$
$$bH = tH = \{b, t\},$$
$$cH = uH = \{c, u\}.$$

Observe that they have the following properties, corresponding to the properties listed in Proposition E3.

(a) $e \in eH$, $r \in rH$, $a \in aH$, and so on.

(b) One of the left cosets, namely $eH$ (equal also to $rH$), is $H$ itself.

(c) Any two left cosets are either the same set or are disjoint.

(d) Each left coset has two elements, the same number of elements as $H$.

## Proof of Proposition E3

(a) Let $g \in G$. Then $g$ lies in the left coset $gH$, because

$$g = ge$$

and $e \in H$ since $H$ is a subgroup.

(b) The subgroup $H$ is a left coset of $H$ because

$$eH = \{eh : h \in H\} = \{h : h \in H\} = H.$$

(c) This property follows immediately from Theorem E2.

(d) Suppose that $H$ has order $m$, with $H = \{h_1, h_2, \ldots, h_m\}$. Let $g$ be any element of $G$. Then

$$gH = \{gh_1,\ gh_2,\ \ \ldots,\ gh_m\}.$$

The $m$ elements of the left coset $gH$ listed here are all distinct, because the Cancellation Laws (Proposition B15) tell us that if $gh_i = gh_j$ then $h_i = h_j$. Hence $gH$ has $m$ elements, the same number of elements as $H$. ■

## Exercise E38

Using only the properties of left cosets in Proposition E3, list the distinct left cosets of each of the following subgroups $H$ of $S(\square)$.

(a) $H = \{e, a, b, c\}$ (b) $H = \{e\}$ (c) $H = S(\square)$

The properties in Proposition E3 give us the following efficient strategy for partitioning a *finite* group into left cosets.

### Strategy E1

To partition a finite group $G$ into left cosets of a subgroup $H$, do the following.

1. Take $H$ as the first left coset.
2. Choose any element $g \in G$ not yet assigned to a left coset and determine the left coset $gH$ to which $g$ belongs.
3. Repeat step 2 until every element of $G$ has been assigned to a left coset.

Strategy E1 is applied in the next worked exercise, in which the left cosets found in Worked Exercise E11 are found again, but this time more efficiently.

## Worked Exercise E12

Partition the group $S(\square)$ into left cosets of the subgroup $H = \{e, r\}$. (The group table of $S(\square)$ is given as Table 7.)

**Table 7** $S(\square)$

| $\circ$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
| $a$ | $a$ | $b$ | $c$ | $e$ | $s$ | $t$ | $u$ | $r$ |
| $b$ | $b$ | $c$ | $e$ | $a$ | $t$ | $u$ | $r$ | $s$ |
| $c$ | $c$ | $e$ | $a$ | $b$ | $u$ | $r$ | $s$ | $t$ |
| $r$ | $r$ | $u$ | $t$ | $s$ | $e$ | $c$ | $b$ | $a$ |
| $s$ | $s$ | $r$ | $u$ | $t$ | $a$ | $e$ | $c$ | $b$ |
| $t$ | $t$ | $s$ | $r$ | $u$ | $b$ | $a$ | $e$ | $c$ |
| $u$ | $u$ | $t$ | $s$ | $r$ | $c$ | $b$ | $a$ | $e$ |

### Solution

We use Strategy E1.

The left cosets are as follows.

The first left coset is $H$ itself.

$$H = \{e, r\}$$

Now we choose an element not in $H$, say $a$, and find $aH$.

$$aH = \{a \circ e, a \circ r\} = \{a, s\}$$

Next we choose an element not in $H$ or $aH$, say $b$, and find $bH$.

$$bH = \{b \circ e, b \circ r\} = \{b, t\}$$

Now we choose an element not in $H$, $aH$ or $bH$, say $c$, and find $cH$.

$$cH = \{c \circ e, c \circ r\} = \{c, u\}$$

Every element of $S(\square)$ has now been assigned to a left coset.

So the partition into left cosets is

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\}.$$

You can practise applying Strategy E1 in the next two exercises.

## Exercise E39

Write down the elements of the group $U_{20}$, show that $H = \{1, 19\}$ is a subgroup of this group, and partition $U_{20}$ into left cosets of this subgroup.

## Exercise E40

Partition $S(\triangle)$ into left cosets of the subgroup $H = \{e, t\}$. (The group table of $S(\triangle)$ is given as Table 8.)

**Table 8** $S(\triangle)$

| $\circ$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
| $a$ | $a$ | $b$ | $e$ | $t$ | $r$ | $s$ |
| $b$ | $b$ | $e$ | $a$ | $s$ | $t$ | $r$ |
| $r$ | $r$ | $s$ | $t$ | $e$ | $a$ | $b$ |
| $s$ | $s$ | $t$ | $r$ | $b$ | $e$ | $a$ |
| $t$ | $t$ | $r$ | $s$ | $a$ | $b$ | $e$ |

In the next worked exercise a permutation group is partitioned into left cosets.

## Worked Exercise E13

Partition the group $S_3$ into left cosets of the subgroup

$$H = \langle (1,2) \rangle = \{e, (1\ 2)\}.$$

### Solution

We use Strategy E1.

The left cosets are as follows.

The first left coset is $H$ itself.

$$H = \{e, (1\ 2)\}$$

Now we choose an element of $S_3$ not in $H$, say $(1\ 3)$, and find $(1\ 3)H$.

$$\begin{aligned}(1\ 3)H &= \{(1\ 3) \circ e, (1\ 3) \circ (1\ 2)\} \\ &= \{(1\ 3), (1\ 2\ 3)\}\end{aligned}$$

Next we choose an element not in $H$ or $(1\ 3)H$, say $(2\ 3)$, and find $(2\ 3)H$.

$$\begin{aligned}(2\ 3)H &= \{(2\ 3) \circ e, (2\ 3) \circ (1\ 2)\} \\ &= \{(2\ 3), (1\ 3\ 2)\}\end{aligned}$$

Every element of $S_3$ has now been assigned to a left coset.

So the partition of $S_3$ into left cosets of $H$ is

$$\{e, (1\ 2)\}, \quad \{(1\ 3), (1\ 2\ 3)\}, \quad \{(2\ 3), (1\ 3\ 2)\}.$$

## Exercise E41

Partition the alternating group

$$A_4 = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3)\}$$

into left cosets of the subgroup

$$H = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\}.$$

(This set $H$ is a subgroup of $A_4$ because it is a subset of $A_4$ and its elements represent the symmetries of the rectangle, as you saw in Table 3 in Subsection 1.3.)

Left cosets and their properties can be used to provide a very straightforward proof of Lagrange's Theorem, as follows.

### Theorem B68 Lagrange's Theorem

Let $G$ be a finite group and let $H$ be any subgroup of $G$. Then the order of $H$ divides the order of $G$.

**Proof** Let $G$ and $H$ have orders $n$ and $m$, respectively, and let the number of left cosets of $H$ in $G$ be $k$. Each left coset has $m$ elements, and the left cosets form a partition of $G$, so the total number of elements in $G$ is $km$. That is, $n = km$. Hence $m$ divides $n$. ■

Although all the examples of left cosets that you have met in this subsection are left cosets in *finite* groups, the definition of left coset applies to any group, whether it is finite or infinite. All the properties of left cosets that we have obtained, and the proofs of these properties, apply to infinite groups as well as to finite ones, unless stated otherwise. In particular, the left cosets of a subgroup of an infinite group form a partition of the group.

A subgroup of an infinite group may have infinitely many distinct left cosets, or only finitely many: you will meet examples of the second possibility in Subsection 4.3, and an example of the first possibility in the next unit.

Frank Nelson Cole

The term 'coset' was first introduced by the American mathematician George Abram Miller (1863–1951) in 1910. In 1893 Miller had taken up a position at the University of Michigan where he came under the influence of Frank Nelson Cole (1861–1926), and it was Cole who inspired Miller to devote himself to group theory. Cole had been a student of Felix Klein (1849–1925) in Leipzig, and in 1892 published an English translation of the 1882 book on group theory by Eugen Netto (1846–1919). Cole's translation was the first book on group theory in English and it was important for stimulating interest in the subject.

## 4.2 Right cosets

In the previous subsection the *left* coset $gH$ of a subgroup $H$ of a group $(G, \circ)$ was defined to be the set

$$gH = \{gh : h \in H\}.$$

That is, it is the subset of $G$ obtained by composing each element of $H$ with $g$ on the *left*.

*Right* cosets are defined in the same way, but with the composition with $g$ on the right, as below.

### Definition

Let $H$ be a subgroup of a group $G$, and let $g$ be an element of $G$. The **right coset** $Hg$ of $H$ is given by

$$Hg = \{hg : h \in H\}.$$

It is the subset of $G$ obtained by composing each element of $H$ with $g$ on the right.

For example, consider the subgroup $H = \{e, r\}$ of the group $S(\square)$, and the element $a \in S(\square)$. The right coset $Ha$ of $H$ in $S(\square)$ is

$$Ha = \{e, r\}a = \{e \circ a, r \circ a\} = \{a, u\}.$$

In the previous subsection we found all the left cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$. In the next worked exercise we find all the right cosets of the same subgroup.

## Worked Exercise E14

Find all the right cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$. (The group table of $S(\square)$ is given as Table 9.)

### Solution

For each $g \in S(\square)$, we find the right coset $Hg$.

$$He = \{e, r\}e = \{e \circ e, r \circ e\} = \{e, r\},$$
$$Ha = \{e, r\}a = \{e \circ a, r \circ a\} = \{a, u\},$$
$$Hb = \{e, r\}b = \{e \circ b, r \circ b\} = \{b, t\},$$
$$Hc = \{e, r\}c = \{e \circ c, r \circ c\} = \{c, s\},$$
$$Hr = \{e, r\}r = \{e \circ r, r \circ r\} = \{r, e\},$$
$$Hs = \{e, r\}s = \{e \circ s, r \circ s\} = \{s, c\},$$
$$Ht = \{e, r\}t = \{e \circ t, r \circ t\} = \{t, b\},$$
$$Hu = \{e, r\}u = \{e \circ u, r \circ u\} = \{u, a\}.$$

**Table 9** $S(\square)$

| $\circ$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
| $a$ | $a$ | $b$ | $c$ | $e$ | $s$ | $t$ | $u$ | $r$ |
| $b$ | $b$ | $c$ | $e$ | $a$ | $t$ | $u$ | $r$ | $s$ |
| $c$ | $c$ | $e$ | $a$ | $b$ | $u$ | $r$ | $s$ | $t$ |
| $r$ | $r$ | $u$ | $t$ | $s$ | $e$ | $c$ | $b$ | $a$ |
| $s$ | $s$ | $r$ | $u$ | $t$ | $a$ | $e$ | $c$ | $b$ |
| $t$ | $t$ | $s$ | $r$ | $u$ | $b$ | $a$ | $e$ | $c$ |
| $u$ | $u$ | $t$ | $s$ | $r$ | $c$ | $b$ | $a$ | $e$ |

As with left cosets, some of the right cosets found in Worked Exercise E14 turn out to be the same set as each other:

$$He = Hr = \{e, r\},$$
$$Ha = Hu = \{a, u\},$$
$$Hb = Ht = \{b, t\},$$
$$Hc = Hs = \{c, s\}.$$

The *distinct* right cosets of the subgroup $H = \{e, r\}$ in the group $S(\square)$ are

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

Notice also that the right coset $Ha$ of $H = \{e, r\}$ is not the same set as the corresponding left coset $aH$. We found above that

$$Ha = \{e, r\}a = \{e \circ a, r \circ a\} = \{a, u\},$$

whereas we found earlier, in Worked Exercise E11, that

$$aH = a\{e, r\} = \{a \circ e, a \circ r\} = \{a, s\}.$$

So, in general, left cosets and right cosets are different sets.

However, sometimes left and right cosets turn out to be the same set. For example, again for the subgroup $H = \{e, r\}$ of the group $S(\square)$, we found above that

$$Hb = \{e, r\}b = \{e \circ b, r \circ b\} = \{b, t\}$$

and earlier, in Worked Exercise E11, we found that

$$bH = b\{e, r\} = \{b \circ e, b \circ r\} = \{b, t\}.$$

So in this instance $Hb = bH$.

All the results for left cosets that you met in the previous subsection have analogous results for right cosets, as stated below. The proofs of these results are analogues of the proofs for left cosets given earlier, so are omitted here.

### Theorem E4

Let $H$ be a subgroup of a group $G$. Then the distinct right cosets of $H$ in $G$ form a partition of $G$.

### Proposition E5 Properties of right cosets

Let $H$ be a subgroup of a group $G$.

(a) The element $g$ lies in the right coset $Hg$, for each $g \in G$.

(b) One of the right cosets of $H$ in $G$ is $H$ itself.

(c) Any two right cosets $Hg_1$ and $Hg_2$ are either the same set or are disjoint.

(d) If $H$ is finite, then each right coset $Hg$ has the same number of elements as $H$.

We also have the following strategy for finding right cosets in a finite group efficiently, analogous to Strategy E1 for left cosets.

### Strategy E2

To partition a finite group $G$ into right cosets of a subgroup $H$, do the following.

1. Take $H$ as the first right coset.
2. Choose any element $g \in G$ not yet assigned to a right coset and determine the right coset $Hg$ to which $g$ belongs.
3. Repeat step 2 until every element of $G$ has been assigned to a right coset.

This strategy is demonstrated in the next worked exercise, in which the right cosets found in Worked Exercise E14 are found again, but this time more efficiently.

## Worked Exercise E15

Partition the group $S(\square)$ into right cosets of the subgroup $H = \{e, r\}$. (The group table of $S(\square)$ is given as Table 10.)

**Table 10** $S(\square)$

| $\circ$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
| $a$ | $a$ | $b$ | $c$ | $e$ | $s$ | $t$ | $u$ | $r$ |
| $b$ | $b$ | $c$ | $e$ | $a$ | $t$ | $u$ | $r$ | $s$ |
| $c$ | $c$ | $e$ | $a$ | $b$ | $u$ | $r$ | $s$ | $t$ |
| $r$ | $r$ | $u$ | $t$ | $s$ | $e$ | $c$ | $b$ | $a$ |
| $s$ | $s$ | $r$ | $u$ | $t$ | $a$ | $e$ | $c$ | $b$ |
| $t$ | $t$ | $s$ | $r$ | $u$ | $b$ | $a$ | $e$ | $c$ |
| $u$ | $u$ | $t$ | $s$ | $r$ | $c$ | $b$ | $a$ | $e$ |

### Solution

We use Strategy E2.

The right cosets are as follows.

The first right coset is $H$ itself.

$$H = \{e, r\}$$

Now we choose an element of $S(\square)$ not in $H$, say $a$, and find $Ha$.

$$Ha = \{e \circ a, r \circ a\} = \{a, u\}$$

Next we choose an element not in $H$ or $Ha$, say $b$, and find $Hb$.

$$Hb = \{e \circ b, r \circ b\} = \{b, t\}$$

Now we choose an element not in $H$, $Ha$ or $Hb$, say $c$, and find $Hc$.

$$Hc = \{e \circ c, r \circ c\} = \{c, s\}$$

Every element has now been assigned to a right coset.

So the partition of $S(\square)$ into right cosets of $H$ is

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

## Exercise E42

Partition $S(\triangle)$ into right cosets of the subgroup $H = \{e, s\}$. (The group table of $S(\triangle)$ is given as Table 11.)

**Table 11** $S(\triangle)$

| $\circ$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
| $a$ | $a$ | $b$ | $e$ | $t$ | $r$ | $s$ |
| $b$ | $b$ | $e$ | $a$ | $s$ | $t$ | $r$ |
| $r$ | $r$ | $s$ | $t$ | $e$ | $a$ | $b$ |
| $s$ | $s$ | $t$ | $r$ | $b$ | $e$ | $a$ |
| $t$ | $t$ | $r$ | $s$ | $a$ | $b$ | $e$ |

We now have two ways to partition a group into cosets of a subgroup: the partition into left cosets and the partition into right cosets. You have seen that these two partitions may not be the same. For example, in Worked Exercise E12 in the previous subsection we found that the partition of $S(\square)$ into left cosets of the subgroup $\{e, r\}$ is

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\},$$

whereas the partition of $S(\square)$ into right cosets of the same subgroup, which we found in Worked Exercise E15, is

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

These two partitions of $S(\square)$ are shown in Figure 26.

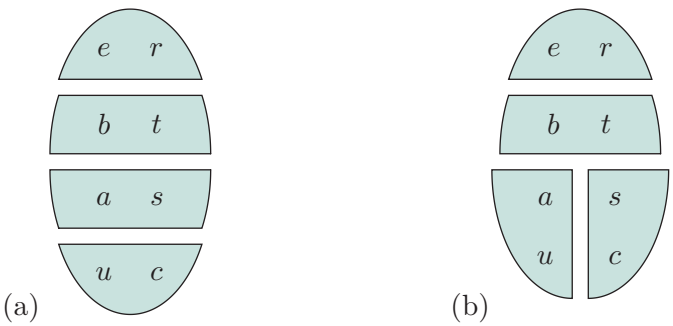



**Figure 26** The partitions of $S(\square)$ into (a) left and (b) right cosets of $\{e, r\}$

Similarly, the partition of $S(\triangle)$ into left cosets of its subgroup $\{e, s\}$, which you were asked to find in Exercise E36 in Subsection 4.1, is

$$\{e, s\}, \quad \{a, r\}, \quad \{b, t\},$$

and this is not the same as the partition of $S(\triangle)$ into right cosets of $\{e, s\}$, which you were asked to find in Exercise E42, and which is

$$\{e, s\}, \quad \{a, t\}, \quad \{b, r\}.$$

These two partitions of $S(\triangle)$ are shown in Figure 27.

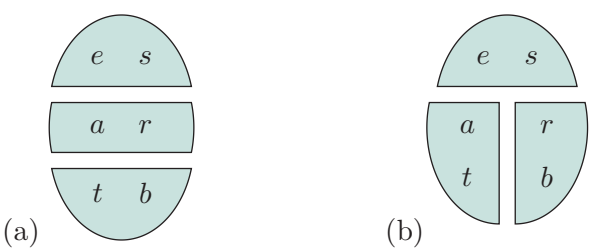



**Figure 27** The partitions of $S(\triangle)$ into (a) left and (b) right cosets of $\{e, s\}$

However, sometimes the partitions of a group into left cosets and right cosets of a subgroup are the same. For example, this always happens if the group is abelian. This is because if $H$ is any subgroup of an abelian group $G$ and $g$ is any element of $G$, then the left coset $gH$ and the right coset $Hg$ are the same set:

$$gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg.$$

The partitions into left cosets and right cosets can also be the same for some groups and subgroups where the group is *non-abelian*. We will consider this possibility in Section 5.

There is in fact a simple connection between the left cosets and the right cosets of a subgroup of a group. If we take the partition into left cosets, and replace every element by its inverse, then we obtain the partition into right cosets, and vice versa.

For example, consider the group $S(\square)$ and its subgroup $\{e, r\}$ again. The partition of $S(\square)$ into left cosets of the subgroup $\{e, r\}$, found in Worked Exercise E12, is

$$\{e, r\}, \quad \{a, s\}, \quad \{b, t\}, \quad \{c, u\}.$$

Let us replace each element in this partition by its inverse. The elements $a$ and $c$ are inverses of each other, and every other element is self-inverse. Replacing each element by its inverse gives the following.

$$\begin{array}{cccc} \{e, r\} & \{a, s\} & \{b, t\} & \{c, u\} \\ \downarrow\downarrow & \downarrow\downarrow & \downarrow\downarrow & \downarrow\downarrow \\ \{e, r\} & \{c, s\} & \{b, t\} & \{a, u\} \end{array}$$

The result is the partition of $S(\square)$ into right cosets of the subgroup $\{e, r\}$, which we found in Worked Exercise E15 to be

$$\{e, r\}, \quad \{a, u\}, \quad \{b, t\}, \quad \{c, s\}.$$

(The order in which the cosets in the partition are listed does not matter, of course.)

This connection between left cosets and right cosets is stated as a theorem below, and you are asked to provide most of the proof as an exercise.

### Theorem E6

Let $H$ be a subgroup of a group $G$.

(a) If every element in the partition of $G$ into left cosets of $H$ is replaced by its inverse, then the result is the partition of $G$ into right cosets of $H$.

(b) The same is true if the words 'left' and 'right' are interchanged.

**Proof** We need to prove only part (a). Part (b) then follows immediately, since the inverse of the inverse of an element is the original element.

To prove part (a), we have to prove that every pair of elements $x$ and $y$ of $G$ lie in the same left coset of $H$ if and only if their inverses $x^{-1}$ and $y^{-1}$ lie in the same right coset of $H$. Now saying that $x$ and $y$ lie in the same left coset of $H$ is the same as saying that $x \in yH$, and similarly saying that $x^{-1}$ and $y^{-1}$ lie in the same right coset of $H$ is the same as saying that $y^{-1} \in Hx^{-1}$. So the fact that we need to prove follows from Exercise E43 below. ■

### Exercise E43

Let $H$ be a subgroup of a group $G$, and let $x, y \in G$. Prove that

$$x \in yH \iff y^{-1} \in Hx^{-1},$$

by proving the $\Longrightarrow$ part and the $\Longleftarrow$ part separately.

Note that Theorem E6 does *not* say that if $H$ is a subgroup of a group $G$ and $g$ is an element of $G$ then replacing every element of the left coset $gH$ by its inverse gives the right coset $Hg$. This procedure certainly gives *a* right coset of $H$ in $G$, by Theorem E6, but it may not be the right coset $Hg$.

Theorem E6 has the following immediate corollary.

### Corollary E7

Let $H$ be a subgroup of a group $G$. Then the number of distinct left cosets of $H$ in $G$ is equal to the number of distinct right cosets of $H$ in $G$ (or there may be infinitely many of each).

We can now make the following definition.

### Definition

The number of distinct left cosets, or, equivalently, the number of distinct right cosets, of a subgroup $H$ in a group $G$ is called the **index** of $H$ in $G$.

If $H$ has infinitely many left cosets, or, equivalently, infinitely many right cosets, in $G$, then we say that $H$ has **infinite index** in $G$.

For example, you saw earlier that the subgroup $H = \{e, r\}$ of the group $S(\square)$ has four left cosets in $S(\square)$ (and also four right cosets), so the index of the subgroup $H = \{e, r\}$ in $S(\square)$ is 4.

It is straightforward to work out the index of a subgroup $H$ in a *finite* group $G$, as follows. (Remember that we use the notation $|G|$ for the order of a finite group $G$.)

### Proposition E8

Let $H$ be a subgroup of a finite group $G$. Then the index of $H$ in $G$ is $|G|/|H|$.

**Proof** This holds because the left cosets (or right cosets) of $H$ partition $G$ and each left coset (and each right coset) has $|H|$ elements. ■

If $H$ is a subgroup of an *infinite* group $G$, then $H$ may have infinitely many left cosets (and hence infinitely many right cosets) in $G$, or only finitely many. That is, $H$ may have infinite index in $G$, or finite index. You will see examples of the second possibility in the next subsection, and examples of the first possibility in the next unit.

## 4.3 Cosets in additive groups

In this subsection we consider cosets in additive groups. Examples of additive groups include $(\mathbb{Z}, +)$ and $(\mathbb{Z}_9, +_9)$.

Since all additive groups are abelian, the left cosets of any subgroup of an additive group are the same as the right cosets. So there is no need to distinguish between left and right cosets, and we refer simply to *cosets*.

For an additive group, we denote cosets using notation of the form $g + H$ rather than $gH$, as follows.

### Convention

Let $H$ be a subgroup of an additive group $(G, +)$, and let $g$ be an element of $G$. The coset $g + H$ of $H$ is the set

$$g + H = \{g + h : h \in H\}.$$

### Worked Exercise E16

Partition the group $\mathbb{Z}_9$ into cosets of the subgroup $H = \langle 3 \rangle = \{0, 3, 6\}$.

### Solution

We use Strategy E1 for partitioning a group into cosets of a subgroup.

The cosets are as follows.

The first coset is $H$ itself.

$$H = \{0, 3, 6\}$$

Now we choose an element not in $H$, say 1, and find $1 + H$.

$$1 + H = \{1 +_9 0,\ 1 +_9 3,\ 1 +_9 6\} = \{1,\ 4,\ 7\}$$

Next we choose an element not in $H$ or $1 + H$, say 2, and find $2 + H$.

$$2 + H = \{2 +_9 0,\ 2 +_9 3,\ 2 +_9 6\} = \{2,\ 5,\ 8\}$$

Every element has now been assigned to a coset.

The partition of $\mathbb{Z}_9$ into cosets of $H$ is therefore

$$\{0, 3, 6\}, \quad \{1, 4, 7\}, \quad \{2, 5, 8\}.$$

## Exercise E44

In each of parts (a) and (b) below, partition the group $\mathbb{Z}_{10}$ into cosets of the subgroup $H$.

(a) $H = \langle 2 \rangle = \{0, 2, 4, 6, 8\}$ (b) $H = \langle 5 \rangle = \{0, 5\}$

Next we look briefly at some examples of partitioning an *infinite* group into cosets of a subgroup. Remember that a subgroup of an infinite group can have infinitely many cosets in the group, or only finitely many: that is, it can have either infinite index or finite index in the group.

If a subgroup has infinite index, then although we could use our usual strategy for finding cosets, Strategy E1, to find more and more of them, we would never find them all. However, if it has finite index, then we can use the strategy to find all the cosets.

In the next worked exercise we use Strategy E1 to partition an infinite additive group into cosets of a subgroup that has finite index.

## Worked Exercise E17

Explain how you know that the set

$$H = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

is a subgroup of the group $(\mathbb{Z}, +)$, and partition $\mathbb{Z}$ into cosets of $H$.

### Solution

The set $H$ is the cyclic subgroup of $(\mathbb{Z}, +)$ generated by 3, so it is a subgroup of $(\mathbb{Z}, +)$.

To find its cosets in $(\mathbb{Z}, +)$, we use Strategy E1.

The cosets are as follows.

The first coset is $H$ itself.

$$H = \{\ldots, -6, -3, 0, 3, 6, \ldots\}$$

We then choose an element not in $H$, say 1, and find $1 + H$.

$$\begin{aligned} 1 + H &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ &= \{\ldots, 1 + (-6), 1 + (-3), 1 + 0, 1 + 3, 1 + 6, \ldots\} \\ &= \{\ldots, -5, -2, 1, 4, 7, \ldots\} \end{aligned}$$

Next we choose an element not in $H$ or $1 + H$, say 2, and find $2 + H$.

$$\begin{aligned} 2 + H &= \{\ldots, -6, -3, 0, 3, 6, \ldots\} \\ &= \{\ldots, 2 + (-6), 2 + (-3), 2 + 0, 2 + 3, 2 + 6, \ldots\} \\ &= \{\ldots, -4, -1, 2, 5, 8, \ldots\} \end{aligned}$$

Every element has now been assigned to a coset.

The partition of $(\mathbb{Z}, +)$ into cosets of $H$ is therefore

$$\begin{aligned} H &= \{\ldots, -6, -3, 0, 3, 6, \ldots\}, \\ 1 + H &= \{\ldots, -5, -2, 1, 4, 7, \ldots\}, \\ 2 + H &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}. \end{aligned}$$

The subgroup $H$ in Worked Exercise E17 is the subset of $\mathbb{Z}$ that we denoted by $3\mathbb{Z}$ in Exercise E33:

$$3\mathbb{Z} = \{3k : k \in \mathbb{Z}\} = \{\ldots, -6, -3, 0, 3, 6, 9, \ldots\}.$$

In general, for any number $x$, we denote the set of integer multiples of $x$ by $x\mathbb{Z}$; that is,

$$x\mathbb{Z} = \{xk : k \in \mathbb{Z}\} = \{\ldots, -2x, -x, 0, x, 2x, 3x, \ldots\}.$$

For any *integer* $n$, the set

$$n\mathbb{Z} = \{nk : k \in \mathbb{Z}\}$$

is a subgroup of $(\mathbb{Z}, +)$, because it is the cyclic subgroup of $(\mathbb{Z}, +)$ generated by $n$.

## Exercise E45

(a) Partition the group $(\mathbb{Z}, +)$ into cosets of the subgroup $4\mathbb{Z}$.

(b) Partition the group $(2\mathbb{Z}, +)$ into cosets of the subgroup $6\mathbb{Z}$.

The blue box below expands on the blue box *Permutations and bell ringing* in Subsection 2.4 of Unit B3. If you want to read it, you may find it helpful to read the earlier box again first. Remember that all the material in the blue boxes is optional.

### Cosets and bell ringing

The blue box *Permutations and bell ringing* in Unit B3 explained that church bell ringers usually ring a sequence of bells in which each bell rings exactly once, then another such sequence with the bells in a different order, then another, and so on, until they have rung a number of such sequences, all different, in some sort of pattern. The order of the sequences in the pattern must be such that each bell changes by at most one place from each sequence to the next.

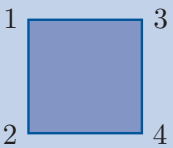
For example, the table below, repeated from Unit B3, shows a suitable pattern for ringing sequences of four bells $A$, $B$, $C$ and $D$.

Bells in the Church of the Assumption of the Blessed Virgin Mary, Leckhampstead, Buckinghamshire

Bell ringers at the Church of the Assumption of the Blessed Virgin Mary, Lillingstone Lovell, Buckinghamshire

The coloured lines trace the changes in place of each bell. The eight sequences of bells are all different, and each bell changes by at most one place from each sequence to the next.

| Sequence of bells | Permutation applied | Permutation from start |
|---|---|---|
| $A\ B\ C\ D$ | | $e$ |
| $B\ A\ D\ C$ | $(1\ 2)(3\ 4)$ | $(1\ 2)(3\ 4)$ |
| $B\ D\ A\ C$ | $(2\ 3)$ | $(1\ 3\ 4\ 2)$ |
| $D\ B\ C\ A$ | $(1\ 2)(3\ 4)$ | $(1\ 4)$ |
| $D\ C\ B\ A$ | $(2\ 3)$ | $(1\ 4)(2\ 3)$ |
| $C\ D\ A\ B$ | $(1\ 2)(3\ 4)$ | $(1\ 3)(2\ 4)$ |
| $C\ A\ D\ B$ | $(2\ 3)$ | $(1\ 2\ 4\ 3)$ |
| $A\ C\ B\ D$ | $(1\ 2)(3\ 4)$ | $(2\ 3)$ |




The column headed 'Permutation applied' in the table shows the permutation of places that is applied to obtain each sequence of bells from the one before. For example, the second sequence $BADC$ is obtained from the first sequence $ABCD$ by interchanging the bells in places 1 and 2 and interchanging the bells in places 3 and 4, that is, by applying the transposition $(1\ 2)(3\ 4)$.

The column headed 'Permutation from start' shows the permutation of places that is applied to obtain each sequence from the *first* sequence. For example, since the second sequence is obtained from the first sequence by applying $(1\ 2)(3\ 4)$, and the third sequence is obtained from the second sequence by applying $(2\ 3)$, it follows that the third sequence is obtained from the first sequence by applying

$$(2\ 3) \circ (1\ 2)(3\ 4) = (1\ 3\ 4\ 2).$$

Similarly, the fourth sequence is obtained from the first sequence by applying

$$(1\ 2)(3\ 4) \circ (1\ 3\ 4\ 2) = (1\ 4),$$

and so on.

Since two sequences of bells are different if and only if the permutations of places applied to obtain them from the first sequence are different, the eight permutations in the 'Permutation from start' column are all different. In fact these eight permutations are the elements of the group $S(\square)$, when the square is labelled as shown on the right above.

A pattern for ringing $n$ bells that contains all possible sequences of the $n$ bells is known as an *extent* for $n$ bells. The pattern in the table above is only a partial extent for four bells, because it contains only

eight sequences whereas the total number of possible sequences for four bells is $4! = 24$. The pattern cannot be extended to a full extent for four bells by continuing it in the same way, that is, by applying the permutations of places $(1\ 2)(3\ 4)$ and $(2\ 3)$ alternately to each new sequence of bells, because applying the permutation $(2\ 3)$ to the eighth sequence gives the first sequence again.

However, the partial extent in the table can be extended to a full extent for four bells by using the idea of *cosets*. Let $H$ be the subgroup of $S_4$ (isomorphic to $S(\square)$) whose elements appear in the 'Permutation from start' column of the table. Each element of $H$ corresponds to a different sequence of bells, as explained above. To extend the partial extent, we disrupt the pattern by applying the transposition $(3\ 4)$ instead of $(2\ 3)$ to the eighth sequence of bells, as shown in the table below. Since the eighth sequence of bells corresponds to the permutation $(2\ 3)$, the ninth sequence of bells then corresponds to the permutation

$$(3\ 4) \circ (2\ 3) = (2\ 4\ 3).$$

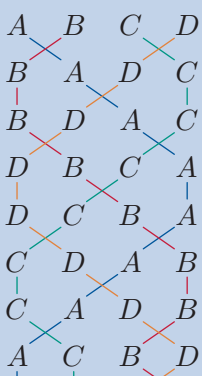
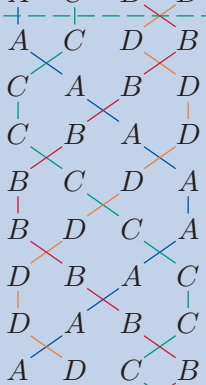
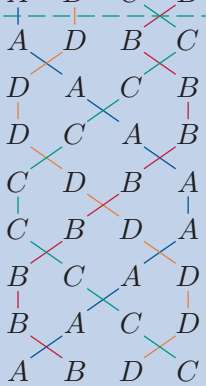
This is not in $H$, so the ninth sequence of bells is different from the first eight sequences. We then continue the pattern in the same way as before, by applying the permutations of places $(1\ 2)(3\ 4)$ and $(2\ 3)$ alternately: a little thought shows that this amounts to composing each of the elements of $H$ in turn on the right by the permutation $(2\ 4\ 3)$, as shown in the table below. So we obtain the eight sequences of bells corresponding to the eight elements of the right coset $H(2\ 4\ 3)$ of $H$ in $S_4$.

We then disrupt the pattern a second time by again applying the transposition $(3\ 4)$. Since the sixteenth sequence of bells corresponds to the permutation $(2\ 3) \circ (2\ 4\ 3)$, the seventeenth sequence of bells then corresponds to the permutation

$$(3\ 4) \circ (2\ 3) \circ (2\ 4\ 3) = (2\ 3\ 4).$$

This is not in $H$ or $H(2\ 4\ 3)$, so the seventeenth sequence of bells is different from the first sixteen sequences. We then continue the pattern in the same way as before, which amounts to composing each of the elements of $H$ in turn on the right by the permutation $(2\ 3\ 4)$, as shown in the table. So we obtain the eight sequences of bells corresponding to the eight elements of the third and final right coset $H(2\ 3\ 4)$ of $H$ in $S_4$.

Since the right cosets of $H$ partition $S_3$, in this way we obtain all 24 different permutations in $S_4$, corresponding to the 24 different sequences of four bells. Notice that applying the 'disrupting' permutation $(3\ 4)$ to the final sequence gives the first sequence again, so bell ringers can ring the extent in the table several times consecutively if they wish.

| Sequence of bells | Permutation applied | Permutation from start | |
|---|---|---|---|
|  | | $e$ | $H$ |
| | $(1\ 2)(3\ 4)$ | $(1\ 2)(3\ 4)$ | |
| | $(2\ 3)$ | $(1\ 3\ 4\ 2)$ | |
| | $(1\ 2)(3\ 4)$ | $(1\ 4)$ | |
| | $(2\ 3)$ | $(1\ 4)(2\ 3)$ | |
| | $(1\ 2)(3\ 4)$ | $(1\ 3)(2\ 4)$ | |
| | $(2\ 3)$ | $(1\ 2\ 4\ 3)$ | |
| | $(1\ 2)(3\ 4)$ | $(2\ 3)$ | |
|  | $(3\ 4)$ | $(2\ 4\ 3)$ | $H(2\ 4\ 3)$ |
| | $(1\ 2)(3\ 4)$ | $(1\ 2)(3\ 4) \circ (2\ 4\ 3)$ | |
| | $(2\ 3)$ | $(1\ 3\ 4\ 2) \circ (2\ 4\ 3)$ | |
| | $(1\ 2)(3\ 4)$ | $(1\ 4) \circ (2\ 4\ 3)$ | |
| | $(2\ 3)$ | $(1\ 4)(2\ 3) \circ (2\ 4\ 3)$ | |
| | $(1\ 2)(3\ 4)$ | $(1\ 3)(2\ 4) \circ (2\ 4\ 3)$ | |
| | $(2\ 3)$ | $(1\ 2\ 4\ 3) \circ (2\ 4\ 3)$ | |
| | $(1\ 2)(3\ 4)$ | $(2\ 3) \circ (2\ 4\ 3)$ | |
|  | $(3\ 4)$ | $(2\ 3\ 4)$ | $H(2\ 3\ 4)$ |
| | $(1\ 2)(3\ 4)$ | $(1\ 2)(3\ 4) \circ (2\ 3\ 4)$ | |
| | $(2\ 3)$ | $(1\ 3\ 4\ 2) \circ (2\ 3\ 4)$ | |
| | $(1\ 2)(3\ 4)$ | $(1\ 4) \circ (2\ 3\ 4)$ | |
| | $(2\ 3)$ | $(1\ 4)(2\ 3) \circ (2\ 3\ 4)$ | |
| | $(1\ 2)(3\ 4)$ | $(1\ 3)(2\ 4) \circ (2\ 3\ 4)$ | |
| | $(2\ 3)$ | $(1\ 2\ 4\ 3) \circ (2\ 3\ 4)$ | |
| | $(1\ 2)(3\ 4)$ | $(2\ 3) \circ (2\ 3\ 4)$ | |

The pattern of eight sequences of four bells in the first table in this blue box is known to bell ringers as *plain hunt minimus*, and the pattern of 24 sequences in the second table is known as *plain bob minimus*. The word 'minimus' indicates that the pattern is rung on four bells.

# 5 Normal subgroups

In the previous section you saw that the partition of a group into left cosets of a particular subgroup may be different from its partition into right cosets of the same subgroup. You saw that if the group is abelian then the two partitions are the same.

There are also some *non-abelian* groups and subgroups for which the two partitions are the same, as illustrated by the following worked exercise.

## Worked Exercise E18

Show that the partition of $S(\square)$ into left cosets of the subgroup $H = \{e, b\}$ is the same as its partition into right cosets of this subgroup. (The group table of $S(\square)$ is given as Table 12.)

**Table 12** $S(\square)$

| $\circ$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
|---|---|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $c$ | $r$ | $s$ | $t$ | $u$ |
| $a$ | $a$ | $b$ | $c$ | $e$ | $s$ | $t$ | $u$ | $r$ |
| $b$ | $b$ | $c$ | $e$ | $a$ | $t$ | $u$ | $r$ | $s$ |
| $c$ | $c$ | $e$ | $a$ | $b$ | $u$ | $r$ | $s$ | $t$ |
| $r$ | $r$ | $u$ | $t$ | $s$ | $e$ | $c$ | $b$ | $a$ |
| $s$ | $s$ | $r$ | $u$ | $t$ | $a$ | $e$ | $c$ | $b$ |
| $t$ | $t$ | $s$ | $r$ | $u$ | $b$ | $a$ | $e$ | $c$ |
| $u$ | $u$ | $t$ | $s$ | $r$ | $c$ | $b$ | $a$ | $e$ |

### Solution

First we find the partition into left cosets, using Strategy E1.

The left cosets are as follows.

$$\begin{aligned} H &= \{e, b\} \\ aH &= \{a \circ e, a \circ b\} = \{a, c\} \\ rH &= \{r \circ e, r \circ b\} = \{r, t\} \\ sH &= \{s \circ e, s \circ b\} = \{s, u\} \end{aligned}$$

So the partition into left cosets is

$$\{e, b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

To find the partition into right cosets, we could use Strategy E2, the right coset analogue of Strategy E1. However, it is quicker to use Theorem E6: to obtain the partition into right cosets we replace each element in the partition into left cosets by its inverse.

In $S(\square)$ the elements $a$ and $c$ are inverses of each other and all the other elements are self-inverse. So the partition into right cosets is

$$\{e, b\}, \quad \{c, a\}, \quad \{r, t\}, \quad \{s, u\},$$

that is,

$$\{e, b\}, \quad \{a, c\}, \quad \{r, t\}, \quad \{s, u\}.$$

Thus the partitions into left cosets and right cosets are the same.

We make the following definition.

### Definition

Let $G$ be a group and let $H$ be a subgroup of $G$. Then $H$ is a **normal subgroup** of $G$ if the partition of $G$ into left cosets of $H$ is the same as the partition of $G$ into right cosets of $H$. We also say that $H$ is **normal in** $G$.

For example, Worked Exercise E18 shows that $\{e, b\}$ is a normal subgroup of $S(\square)$.

On the other hand, the subgroup $\{e, r\}$ of $S(\square)$ is *not* a normal subgroup of $S(\square)$, because, as you saw in Worked Exercises E12 and E15, for this subgroup the partitions into left cosets and right cosets are different.

Normal subgroups play an important role in group theory, as you will see throughout the rest of this book. Some texts use the notation $H \lhd G$ to assert that $H$ is a normal subgroup of $G$, but we will not use this notation in this module.

## Exercise E46

Determine whether each of the following subgroups of $S(\triangle)$ is normal.

(a) $\langle t \rangle = \{e, t\}$ (b) $S^+(\triangle) = \{e, a, b\}$ (c) $\{e\}$ (d) $S(\triangle)$

**Table 13** $S(\triangle)$

| $\circ$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
|---|---|---|---|---|---|---|
| $e$ | $e$ | $a$ | $b$ | $r$ | $s$ | $t$ |
| $a$ | $a$ | $b$ | $e$ | $t$ | $r$ | $s$ |
| $b$ | $b$ | $e$ | $a$ | $s$ | $t$ | $r$ |
| $r$ | $r$ | $s$ | $t$ | $e$ | $a$ | $b$ |
| $s$ | $s$ | $t$ | $r$ | $b$ | $e$ | $a$ |
| $t$ | $t$ | $r$ | $s$ | $a$ | $b$ | $e$ |

(The group table of $S(\triangle)$ is given as Table 13. In Exercise E40 in Subsection 4.1 you were asked to partition $S(\triangle)$ into left cosets of the subgroup $\langle t \rangle = \{e, t\}$.)

## Exercise E47

Consider the alternating group

$$A_4 = \{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3),\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3)\}.$$

(a) Let $H$ be the subgroup $\{e, (1\ 2\ 3), (1\ 3\ 2)\}$ of $A_4$ (it is the cyclic subgroup generated by $(1\ 2\ 3)$).

By finding the left coset $(1\ 2)(3\ 4)H$ and right coset $H(1\ 2)(3\ 4)$, show that $H$ is not a normal subgroup of $A_4$.

(b) Let $K$ be the subgroup $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ of $A_4$. (It is the subgroup of $S_4$ that represents the symmetries of the rectangle when its vertices are labelled 1, 2, 3 and 4.)

Show that $K$ is a normal subgroup of $A_4$.

(You were asked to partition $A_4$ into left cosets of this subgroup in Exercise E41 in Subsection 4.1.)

As illustrated by Exercise E46(c) and (d), every group has at least two normal subgroups, as follows.

### Theorem E9

The following are normal subgroups of any group $G$.

(a) The trivial subgroup $\{e\}$.

(b) The whole group $G$.

**Proof** Let $G$ be any group.

(a) Every left coset and every right coset of $\{e\}$ in $G$ contains just one element. So the partition of $G$ into left cosets of $\{e\}$ is the same as the partition of $G$ into right cosets of $\{e\}$. That is, $\{e\}$ is a normal subgroup of $G$.

(b) There is only one left coset of $G$ in $G$, namely $G$ itself, and similarly there is only one right coset of $G$ in $G$, namely $G$ itself. Thus the partition of $G$ into left cosets of $G$ is the same as the partition of $G$ into right cosets of $G$. That is, $G$ is a normal subgroup of $G$. ■

For some groups, the subgroups in Theorem E9 are its *only* normal subgroups. At the other extreme, there are groups in which *every* subgroup is normal. For example, this is the case for every abelian group, as you saw in Subsection 4.2. This is stated and proved formally below.

### Theorem E10

In an abelian group, every subgroup is normal.

**Proof** Let $H$ be any subgroup of an abelian group $G$, and let $g$ be any element of $G$. Then the left coset $gH$ and the right coset $Hg$ are the same set:

$$gH = \{gh : h \in H\} = \{hg : h \in H\} = Hg.$$

Thus the partitions of $G$ into left cosets and right cosets of $H$ are the same. Hence $H$ is normal in $G$. ■

There is another straightforward situation in which a subgroup of a group is guaranteed to be a normal subgroup. This is when the subgroup has exactly two left cosets, or, equivalently, exactly two right cosets. This was the case in Exercise E46(b), for example, in which you saw that $S^+(\triangle) = \{e, a, b\}$ is a normal subgroup of $S(\triangle)$ because the partitions into left cosets and right cosets are both as follows:

$$\{e, a, b\}, \quad \{r, s, t\}.$$

The general result is stated as the next theorem, using the term *index*. Remember that the index of a subgroup in a group is the number of left cosets, or, equivalently, the number of right cosets, that it has in the group. The number of left cosets is always equal to the number of right cosets by Corollary E7.

### Theorem E11

Every subgroup of index 2 in a group is a normal subgroup of the group.

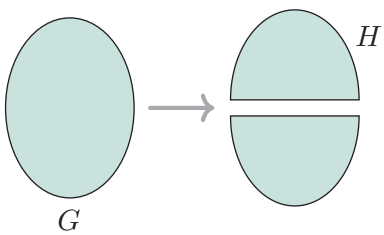



**Figure 28** A group $G$ partitioned into two cosets of a subgroup $H$

**Proof** Let $H$ be a subgroup of index 2 in a group $G$; that is, $H$ has exactly two left cosets and exactly two right cosets in $G$. Then the partition of $G$ into left cosets of $H$ and the partition of $G$ into right cosets of $H$ must each consist of the subgroup itself and a second coset containing all the elements of $G$ that are not in $H$, as illustrated in Figure 28. Thus the two partitions are the same, so $H$ is a normal subgroup of $G$. ■

A subgroup of index 2 in a *finite* group $G$ is simply a subgroup whose order is half of the order of $G$. However, an infinite group can also have a subgroup of index 2.

The following result about symmetric groups follows from Theorem E11.

### Corollary E12

For each positive integer $n$, the alternating group $A_n$ is a normal subgroup of the symmetric group $S_n$.

**Proof** For $n \geq 2$, this follows from the facts that the order of $S_n$ is $n!$ and the order of $A_n$ is $n!/2$. (See Theorems B53 and B62, restated in Subsection 1.2.) For $n = 1$ it follows from the fact that $A_1 = S_1$. ■

### Exercise E48

Explain how you know that each of the following subgroups is normal in the stated group.

(a) The subgroup $4\mathbb{Z}$ of the group $(\mathbb{Z}, +)$.

(b) The subgroup of direct symmetries of the group $S(\text{tet})$ (the symmetry group of the regular tetrahedron).

(c) The subgroup of direct symmetries of the group $S(\clubsuit)$ (the symmetry group of the 4-windmill).

As you have seen, the condition for a subgroup $H$ of a group $G$ to be a normal subgroup of $G$ is that the partition of $G$ into left cosets of $H$ must be the same as the partition of $G$ into right cosets of $H$. This condition can be expressed algebraically, as stated in the proposition below.

### Proposition E13

Let $H$ be a subgroup of a group $G$. Then $H$ is normal in $G$ if and only if

$$gH = Hg$$

for each element $g \in G$.

### Proof

**'If' part**

Suppose that $gH = Hg$ for each element $g \in G$. It follows immediately that the partitions of $G$ into left cosets and right cosets of $H$ are the same, so $H$ is normal in $G$.

**'Only if' part**

Suppose that $H$ is normal in $G$. Let $g$ be any element of $G$. Then $gH$ is the left coset containing $g$, and $Hg$ is the right coset containing $g$. Since $H$ is normal, the partitions of $G$ into left cosets and right cosets of $H$ are the same, so we must have $gH = Hg$. ■

It is important to appreciate that the equation $gH = Hg$ in Proposition E13 means that the sets $gH$ and $Hg$ *contain the same elements*: it does not mean that $gh = hg$ for all $h \in H$. For example, for the subgroup $H = S^+(\triangle) = \{e, a, b\}$ of $S(\triangle)$, we have

$$rH = \{r \circ e,\ r \circ a,\ r \circ b\} = \{r, s, t\},$$
$$Hr = \{e \circ r,\ a \circ r,\ b \circ r\} = \{r, t, s\}.$$

These *sets* are the same, so $rH = Hr$, but, for example,

$$r \circ a = s, \quad \text{whereas} \quad a \circ r = t.$$

If $N$ is a normal subgroup of a group $G$ then, since the left cosets of $N$ are the same as the right cosets of $N$, we can refer simply to the *cosets* of $N$, in the same way as we do for subgroups of abelian groups. We will do this throughout the remainder of this book whenever we work with cosets of normal subgroups.

# Summary

In this unit you revised many of the fundamental ideas of group theory that you met in Book B. You should now be ready to build on them to understand the deeper group theory in this book. You also met a new family of groups, namely the subgroups of the *general linear group of degree 2*, the group of all invertible $2 \times 2$ matrices under matrix multiplication. You started your study of more advanced group theory by meeting the ideas of the *left cosets* and the *right cosets* of a subgroup of a group. You saw that the left cosets of a subgroup of a group are subsets of the group that are 'shifts' of the subgroup and that they partition the group, and you saw that the right cosets of the subgroup are similar. You met *normal subgroups*, subgroups for which the partition into left cosets is the same as the partition into right cosets.

Starting in the next unit, you will see how the ideas of cosets and normal subgroups lead us to the concept of *quotient groups*, which is a powerful tool for gaining a deeper understanding of the structures of groups.

# Learning outcomes

After working through this unit, you should be able to:

- work fluently with the ideas and techniques from Book B revised in this unit
- determine whether a given set of $2 \times 2$ matrices forms a group under matrix multiplication
- determine the *left cosets* and the *right cosets* of a subgroup in a group
- understand that the left cosets and the right cosets of a subgroup in a group each form a *partition* of the group, and determine such partitions
- determine whether a subgroup of a group is a *normal* subgroup of the group.

# Solutions to exercises

## Solution to Exercise E1

**(a)** We check the group axioms for $(A, +)$.

**G1** Let $g, h \in A$. Then $g = 5m$ and $h = 5n$ for some integers $m$, $n$. Hence

$$g + h = 5m + 5n = 5(m + n).$$

Since $m + n$ is an integer, this shows that $g + h \in A$. Thus $A$ is closed under addition.

**G2** Addition of integers is associative.

**G3** We have $0 \in A$, and for all $g \in A$,

$$g + 0 = g = 0 + g.$$

So 0 is an identity element for $+$ on $A$.

**G4** Let $g \in A$. Then $g = 5m$ for some integer $m$. Now

$$-g = -(5m) = 5(-m).$$

Since $-m$ is an integer, this shows that $-g \in A$. Also

$$g + (-g) = 0 = -g + g.$$

Thus each element of $A$ has an inverse in $A$ with respect to addition.

Hence $(A, +)$ satisfies the four group axioms, and so is a group.

**(b)** We check the group axioms for $(A, \times)$.

**G1** Let $g, h \in A$. Then $g = 5m$ and $h = 5n$ for some integers $m$, $n$. Hence

$$g \times h = 5m \times 5n = 5(5mn).$$

Since $5mn$ is an integer, this shows that $g \times h \in A$. Thus $A$ is closed under multiplication.

**G2** Multiplication of integers is associative.

**G3** Since $1 \notin A$, there is no element $e \in A$ such that

$$g \times e = g = e \times g$$

for all $g \in A$. So there is no identity element for $\times$ on $A$.

Hence $(A, \times)$ does not satisfy axiom G3, so it is not a group.

(It is not necessary to confirm that axioms G1 and G2 are satisfied here: you can just show that axiom G3 is not satisfied.)

## Solution to Exercise E2

We check the group axioms for $\big([0, 1), +_1\big)$.

**G1** Let $x, y \in [0, 1)$. By the definition of the binary operation $+_1$,

$$x +_1 y \in [0, 1).$$

Thus $[0, 1)$ is closed under $+_1$.

**G2** We are given that $+_1$ is associative on $[0, 1)$.

**G3** We have $0 \in [0, 1)$, and for all $x \in [0, 1)$,

$$\begin{aligned} x +_1 0 &= \mathrm{frac}(x + 0) \\ &= \mathrm{frac}(x) \\ &= x \quad (\text{since } x \in [0, 1)), \end{aligned}$$

and similarly

$$0 +_1 x = x.$$

Thus 0 is an identity element for $+_1$ on $[0, 1)$.

**G4** The element 0 of $[0, 1)$ has inverse 0 with respect to $+_1$, since

$$0 +_1 0 = 0.$$

Now let $x$ be any other element of $[0, 1)$. Then $1 - x \in [0, 1)$ and we have

$$\begin{aligned} x +_1 (1 - x) &= \mathrm{frac}(x + (1 - x)) \\ &= \mathrm{frac}(1) \\ &= 0, \end{aligned}$$

and similarly

$$(1 - x) +_1 x = 0.$$

Hence $1 - x$ is an inverse of $x$ with respect to $+_1$.

Thus each element of $[0, 1)$ has an inverse in $[0, 1)$ with respect to $+_1$.

Therefore $([0, 1), +_1)$ satisfies the four group axioms, and so is a group.

(Proving that $+_1$ is associative on $[0, 1)$ is trickier than checking the other three group axioms for $\big([0, 1), +_1\big)$, but it can be done as follows.

**G2** By the definition of $+_1$, if $x$ and $y$ are any elements of $[0, 1)$ then

$$\begin{aligned} x +_1 y &= \text{frac}(x + y) \\ &= x + y - \lfloor x + y \rfloor, \end{aligned}$$

so $x +_1 y$ is equal to $x + y$ minus some integer.

Now let $x, y, z \in [0, 1)$. Then

$$\begin{aligned} &(x +_1 y) +_1 z \\ &= (x + y - p) +_1 z \quad \text{where } p \in \mathbb{Z} \\ &= (x + y - p) + z - q \quad \text{where } q \in \mathbb{Z} \\ &= x + y + z - (p + q). \end{aligned}$$

Similarly,

$$\begin{aligned} &x +_1 (y +_1 z) \\ &= x +_1 (y + z - r) \quad \text{where } r \in \mathbb{Z} \\ &= x + (y + z - r) - s \quad \text{where } s \in \mathbb{Z} \\ &= x + y + z - (r + s). \end{aligned}$$

Since $(x +_1 y) +_1 z$ and $x +_1 (y +_1 z)$ both lie in the interval $[0, 1)$, the integers $p + q$ and $r + s$ in the final lines of the two manipulations above must be the *same* integer. Therefore

$$(x +_1 y) +_1 z = x +_1 (y +_1 z).$$

Thus $+_1$ is associative on $[0, 1)$.)

## Solution to Exercise E3

We construct the Cayley table for $(G, \times)$ by multiplying each pair of the matrices $\mathbf{I}$, $\mathbf{R}$, $\mathbf{S}$, $\mathbf{T}$ individually. The table is as follows.

| $\times$ | $\mathbf{I}$ | $\mathbf{R}$ | $\mathbf{S}$ | $\mathbf{T}$ |
|---|---|---|---|---|
| $\mathbf{I}$ | $\mathbf{I}$ | $\mathbf{R}$ | $\mathbf{S}$ | $\mathbf{T}$ |
| $\mathbf{R}$ | $\mathbf{R}$ | $\mathbf{I}$ | $\mathbf{T}$ | $\mathbf{S}$ |
| $\mathbf{S}$ | $\mathbf{S}$ | $\mathbf{T}$ | $\mathbf{I}$ | $\mathbf{R}$ |
| $\mathbf{T}$ | $\mathbf{T}$ | $\mathbf{S}$ | $\mathbf{R}$ | $\mathbf{I}$ |

We consider each axiom in turn.

**G1** Every element in the body of the table is in $G$, so $G$ is closed under matrix multiplication.

**G2** Matrix multiplication is associative.

**G3** The table shows that the matrix $\mathbf{I}$ is an identity element for $(G, \times)$.

**G4** The table shows that all the matrices in $G$ are self-inverse.

Since all four axioms hold, $(G, \times)$ is a group.

The Cayley table is symmetric with respect to the main diagonal, so $(G, \times)$ is an abelian group.

## Solution to Exercise E4

**(a)** A Cayley table for $(\{0, 1, 2\}, +_3)$ is as follows.

| $+_3$ | 0 | 1 | 2 |
|---|---|---|---|
| 0 | 0 | 1 | 2 |
| 1 | 1 | 2 | 0 |
| 2 | 2 | 0 | 1 |

We consider each axiom in turn.

**G1** Every element in the body of the table is in $\{0, 1, 2\}$, so $\{0, 1, 2\}$ is closed under $+_3$.

**G2** Modular addition is associative.

**G3** The table shows that 0 is an identity element for $+_3$ on $\{0, 1, 2\}$.

**G4** The table shows that 0 is self-inverse, and 1 and 2 are inverses of each other.

Since all four axioms hold, $(\{0, 1, 2\}, +_3)$ is a group.

**(b)** A Cayley table for $(\{2, 4, 6\}, \times_8)$ is as follows.

| $\times_8$ | 2 | 4 | 6 |
|---|---|---|---|
| 2 | 4 | 0 | 4 |
| 4 | 0 | 0 | 0 |
| 6 | 4 | 0 | 4 |

The integer 0 appears in the body of the table, but $0 \notin \{2, 4, 6\}$, so $\{2, 4, 6\}$ is not closed under $\times_8$. Thus axiom G1 (closure) does not hold, so $(\{2, 4, 6\}, \times_8)$ is not a group.

**(c)** A Cayley table for $(\{1, 5\}, \times_6)$ is as follows.

| $\times_6$ | 1 | 5 |
|---|---|---|
| 1 | 1 | 5 |
| 5 | 5 | 1 |

We consider each axiom in turn.

**G1** Every element in the body of the table is in $\{1, 5\}$, so $\{1, 5\}$ is closed under $\times_6$.

**G2** Modular multiplication is associative.

**G3** The table shows that 1 is an identity element for $\times_6$ on $\{1, 5\}$.

**G4** The table shows that 1 and 5 are both self-inverse.

Since all four axioms hold, $(\{1, 5\}, \times_6)$ is a group.

**(d)** A Cayley table for $(\{3,9,15,21\},\times_{24})$ is as follows.

| $\times_{24}$ | 3 | 9 | 15 | 21 |
|---|---|---|---|---|
| 3 | 9 | 3 | 21 | 15 |
| 9 | 3 | 9 | 15 | 21 |
| 15 | 21 | 15 | 9 | 3 |
| 21 | 15 | 21 | 3 | 9 |

We consider each axiom in turn.

**G1** Every element in the body of the table is in $\{3,9,15,21\}$, so $\{3,9,15,21\}$ is closed under $\times_{24}$.

**G2** Modular multiplication is associative.

**G3** The table shows that 9 is an identity element for $\times_{24}$ on $\{3,9,15,21\}$.

**G4** The table shows that all four elements of $(\{3,9,15,21\},\times_{24})$ are self-inverse.

Since all four axioms hold, $(\{3,9,15,21\},\times_{24})$ is a group.

## Solution to Exercise E5

**(a)** $U_{18}=\{1,5,7,11,13,17\}$

**(b)** $U_7=\{1,2,3,4,5,6\}$

**(c)** $\mathbb{Z}_7^*=\{1,2,3,4,5,6\}=U_7$

## Solution to Exercise E6

**(a)** $(1\ 2\ 7\ 5)(3\ 8\ 4)\circ(1\ 3\ 6\ 7\ 5)$
$=(1\ 8\ 4\ 3\ 6\ 5\ 2\ 7)$

**(b)** $(1\ 3\ 7)(2\ 5\ 4)\circ(2\ 4)(3\ 8)(5\ 6)$
$=(1\ 3\ 8\ 7)(2)(4\ 5\ 6)$
$=(1\ 3\ 8\ 7)(4\ 5\ 6)$

## Solution to Exercise E7

$(1\ 4\ 5\ 6)\circ(2\ 3\ 7\ 4\ 8)\circ(1\ 7\ 6)(3\ 2\ 5)$
$=(1\ 5\ 7)(2\ 6\ 4\ 8)(3)$
$=(1\ 5\ 7)(2\ 6\ 4\ 8)$

## Solution to Exercise E8

**(a)** $((1\ 7\ 5\ 2)(3\ 8\ 4))^{-1}$
$=(2\ 5\ 7\ 1)(4\ 8\ 3)$
$=(1\ 2\ 5\ 7)(3\ 4\ 8)$ (more usual form)

**(b)** $((1\ 4)(2\ 3)(6\ 8))^{-1}$
$=(4\ 1)(3\ 2)(8\ 6)$
$=(1\ 4)(2\ 3)(6\ 8)$ (more usual form)

(In general, a permutation that contains only cycles of lengths 2 or 1 is self-inverse.)

## Solution to Exercise E9

$(1\ 5\ 3)(2\ 4\ 7\ 9\ 6)$
$=(1\ 3)\circ(1\ 5)\circ(2\ 6)\circ(2\ 9)\circ(2\ 7)\circ(2\ 4)$

## Solution to Exercise E10

**(a)** The parity of $(1\ 5\ 8)(2\ 7\ 3\ 4)$ is

even + odd = odd.

**(b)** The parity of $(1\ 8)(2\ 7)(3\ 5\ 4\ 6)$ is

odd + odd + odd = odd.

## Solution to Exercise E11

**(a)** $a\circ s=r$

**(b)** $b^{-1}=a$

(We look along the row labelled $b$ until we find $e$, then note that it is in the column labelled $a$.)

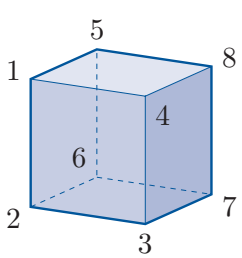
**(c)** Working from the right, we obtain

$$b\circ r\circ a=b\circ(r\circ a)=b\circ s=t.$$

Alternatively, working from the left, we obtain

$$b\circ r\circ a=(b\circ r)\circ a=s\circ a=t.$$

## Solution to Exercise E12




**(a)** **(i)** The permutation $(1\ 8)(2\ 7)$ represents the reflection of the cube in the plane 3456.

**(ii)** The permutation $(1\ 4\ 8\ 5)(2\ 3\ 7\ 6)$ represents a rotation of the cube through $\pi/2$ about the vertical axis of symmetry of the cube. The rotation is anticlockwise when we look down this axis of symmetry from above.

**(b)** We have

$$(1\ 8)(2\ 7) \circ (1\ 4\ 8\ 5)(2\ 3\ 7\ 6) = (1\ 4)(2\ 3)(5\ 8)(6\ 7)$$

and

$$(1\ 4\ 8\ 5)(2\ 3\ 7\ 6) \circ (1\ 8)(2\ 7) = (1\ 5)(2\ 6)(3\ 7)(4\ 8).$$

The first of these permutations is the reflection in the plane that bisects the edges 14, 23, 58 and 67. The second is the reflection in the plane that bisects the edges 15, 26, 37 and 48.

**(c) (i)** The rotation through $\pi$ about the line through the midpoints of the faces 1265 and 4378 is represented by $(1\ 6)(2\ 5)(3\ 8)(4\ 7)$.

**(ii)** The two non-trivial rotations about the line through the vertices 1 and 7 are represented by $(2\ 4\ 5)(3\ 8\ 6)$ and $(2\ 5\ 4)(3\ 6\ 8)$.

## Solution to Exercise E13

**(a)** The integers 5, 10, 15 and 20 are not coprime to 25, so the set $A$ is not a subset of $U_{25}$ and hence it is not a subgroup of the group $(U_{25}, \times_{25})$.

**(b)** We have $B = \{1, 6, 11, 16, 21\} \subseteq U_{25}$, and the binary operation $\times_{25}$ is the same on each set.

The Cayley table for $(B, \times_{25})$ is as follows.

| $\times_{25}$ | 1 | 6 | 11 | 16 | 21 |
|---|---|---|---|---|---|
| 1 | 1 | 6 | 11 | 16 | 21 |
| 6 | 6 | 11 | 16 | 21 | 1 |
| 11 | 11 | 16 | 21 | 1 | 6 |
| 16 | 16 | 21 | 1 | 6 | 11 |
| 21 | 21 | 1 | 6 | 11 | 16 |

We check the three subgroup properties.

**SG1** Every element in the body of the table is in $B$, so $B$ is closed under $\times_{25}$.

**SG2** The identity element in $(U_{25}, \times_{25})$ is 1, and we have $1 \in B$.

**SG3** The Cayley table shows that the element 1 is self-inverse, the elements 6 and 21 are inverses of each other, and the elements 11 and 16 are inverses of each other. So $B$ contains the inverse of each of its elements.

Hence $B$ satisfies the three subgroup properties and so is a subgroup of $(U_{25}, \times_{25})$.

**(c)** The integers 9 and 11 are in $C$, but

$$9 \times_{25} 11 = 24 \notin C,$$

so $C$ is not closed under $\times_{25}$. That is, property SG1 fails.

Hence $C$ is not a subgroup of $(U_{25}, \times_{25})$.

## Solution to Exercise E14

The set $\{e, x\}$ is a subset of $G$. Since $e$ is the identity element of $(G, \circ)$ and $x$ is self-inverse, the Cayley table for $(\{e, x\}, \circ)$ is as follows.

| $\circ$ | $e$ | $x$ |
|---|---|---|
| $e$ | $e$ | $x$ |
| $x$ | $x$ | $e$ |

We check the three subgroup properties.

**SG1** Every element in the body of the table is in $\{e, x\}$, so this set is closed under $\circ$.

**SG2** The identity element in $(G, \circ)$ is $e$, and we have $e \in \{e, x\}$.

**SG3** The elements $e$ and $x$ are both self-inverse, so $\{e, x\}$ contains the inverse of each of its elements.

Hence $\{e, x\}$ satisfies the three subgroup properties and so is a subgroup of $(G, \circ)$.

## Solution to Exercise E15

**(a)** The subgroup of order 1 is $\{e\}$.

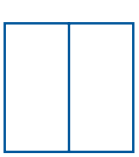
**(b)** The five subgroups of order 2 are

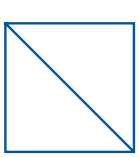
$$\{e, b\}, \quad \{e, r\}, \quad \{e, s\}, \quad \{e, t\}, \quad \{e, u\}.$$

**(c)** The three subgroups of order 4 are

$$\{e, a, b, c\}, \quad \{e, b, r, t\}, \quad \{e, b, s, u\}.$$

The first of these is the group of rotations (direct symmetries) of the square; it can be spotted in the top left-hand corner of the group table for $S(\square)$. The subgroups $\{e, b, r, t\}$ and $\{e, b, s, u\}$ can be obtained by considering the symmetries of each of the following modified squares, respectively.





**(d)** The subgroup of order 8 is $S(\square)$ itself.

## Solution to Exercise E16

The subgroup of $S_7$ obtained from the figure is

$$\{e, (1\ 3\ 7), (1\ 7\ 3), (1\ 3), (1\ 7), (3\ 7)\}.$$

## Solution to Exercise E17

**(a)** We show that the three subgroup properties hold for $G$.

**SG1** Let $f, g \in G$. Then both $f$ and $g$ map each element of $A$ to another element of $A$. We have to show that $f \circ g$ maps each element of $A$ to another element of $A$. To do this, let $k \in A$. Then $g(k) \in A$ and hence $f(g(k)) \in A$, that is $(f \circ g)(k) \in A$. Thus $f \circ g$ maps each element of $A$ to another element of $A$, so $f \circ g \in G$. Thus property SG1 holds.

**SG2** The identity permutation $e$ in $S_n$ maps each element of $A$ to itself, so $e \in G$. Thus property SG2 holds.

**SG3** Let $f \in G$. Then $f$ maps each element of $A$ to another element of $A$. We have to show that $f^{-1}$ maps each element of $A$ to another element of $A$. Since $f$ is one-to-one and maps each element of the finite set $A$ to another element of $A$, each element of $A$ must occur as the image of an element of $A$ under $f$. Hence the image of each element of $A$ under $f^{-1}$ is an element of $A$, as required. Thus property SG3 holds.

Hence $G$ is a subgroup of $S_n$.

**(b)** When $n = 5$ and $A = \{4, 5\}$ the elements of the group $G$ defined in part (a) are as follows:

$$\begin{array}{ll} e, & (4\ 5), \\ (1\ 2\ 3), & (1\ 2\ 3)(4\ 5), \\ (1\ 3\ 2), & (1\ 3\ 2)(4\ 5), \\ (1\ 2), & (1\ 2)(4\ 5), \\ (1\ 3), & (1\ 3)(4\ 5), \\ (2\ 3), & (2\ 3)(4\ 5). \end{array}$$

(This group can also be obtained by labelling the vertices of the double tetrahedron: see Worked Exercise B39 in Unit B3.)

## Solution to Exercise E18

**(a)** This matrix has determinant

$$1 \times 2 - 3 \times 0 = 2 - 0 = 2$$

and so is invertible. Its inverse is

$$\frac{1}{2}\begin{pmatrix} 2 & -3 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -\frac{3}{2} \\ 0 & \frac{1}{2} \end{pmatrix}.$$

**(b)** This matrix is not invertible because it has determinant

$$2 \times (-1) - (-2) \times 1 = -2 + 2 = 0.$$

## Solution to Exercise E19

We show that the three subgroup properties hold for $D$.

**SG1** Let $\mathbf{A}, \mathbf{B} \in D$. Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ 0 & u \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & 0 \\ 0 & y \end{pmatrix},$$

for some $r, u, v, y \in \mathbb{R}$. Hence

$$\mathbf{AB} = \begin{pmatrix} r & 0 \\ 0 & u \end{pmatrix}\begin{pmatrix} v & 0 \\ 0 & y \end{pmatrix} = \begin{pmatrix} rv & 0 \\ 0 & uy \end{pmatrix}.$$

This is a diagonal matrix, so $\mathbf{AB} \in D$. Thus $D$ is closed under matrix multiplication.

(To show that $\mathbf{AB} \in D$ here we do not need to show that $\mathbf{AB} \in \mathrm{GL}(2)$: we know that already because $\mathbf{A}, \mathbf{B} \in \mathrm{GL}(2)$ and $\mathrm{GL}(2)$ is a group. We just need to show that $\mathbf{AB}$ is diagonal.)

**SG2** The identity element $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ of $\mathrm{GL}(2)$ is diagonal. Hence $\mathbf{I} \in D$.

**SG3** Let $\mathbf{A} \in D$. Then

$$\mathbf{A} = \begin{pmatrix} r & 0 \\ 0 & u \end{pmatrix},$$

for some $r, u \in \mathbb{R}$. The inverse of $\mathbf{A}$ in $\mathrm{GL}(2)$ is

$$\mathbf{A}^{-1} = \frac{1}{ru}\begin{pmatrix} u & 0 \\ 0 & r \end{pmatrix} = \begin{pmatrix} 1/r & 0 \\ 0 & 1/u \end{pmatrix}.$$

This is a diagonal matrix, so $\mathbf{A}^{-1} \in D$. Thus $D$ contains the inverse of each of its elements.

(To show that $\mathbf{A}^{-1} \in D$ here we do not need to show that $\mathbf{A}^{-1} \in \mathrm{GL}(2)$: we know that already because $\mathbf{A} \in \mathrm{GL}(2)$ and $\mathrm{GL}(2)$ is a group. We just need to show that $\mathbf{A}^{-1}$ is diagonal.)

Since the three subgroup properties hold, $D$ is a subgroup of $\mathrm{GL}(2)$.

(Since every diagonal matrix is also an upper triangular matrix and a lower triangular matrix, it follows that $D$ is also a subgroup of the group $L$ of invertible $2 \times 2$ lower triangular matrices, and a subgroup of the group $U$ of invertible $2 \times 2$ upper triangular matrices.)

## Solution to Exercise E20

We show that the three subgroup properties hold.

**SG1** Let $\mathbf{A}, \mathbf{B} \in H$. Then $\det \mathbf{A} = 1$ and $\det \mathbf{B} = 1$. Hence

$$\det(\mathbf{AB}) = (\det \mathbf{A})(\det \mathbf{B}) = 1 \times 1 = 1.$$

So $\mathbf{AB} \in H$. Thus $H$ is closed under matrix multiplication.

**SG2** The identity matrix $\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ has determinant $1 \times 1 - 0 \times 0 = 1$, so $\mathbf{I} \in H$.

**SG3** Let $\mathbf{A} \in H$. Then $\det \mathbf{A} = 1$. Hence

$$\det \mathbf{A}^{-1} = 1/(\det \mathbf{A}) = 1/1 = 1.$$

So $\mathbf{A}^{-1} \in H$. Thus $H$ contains the inverse of each of its elements.

Hence $H$ satisfies the three subgroup properties, so it is a subgroup of GL(2).

## Solution to Exercise E21

**(a)** The set $M$ is a subset of the group GL(2), because each matrix

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}, \quad \text{where } a \neq 0,$$

in $M$ has determinant

$$a \times a - b \times 0 = a^2 \neq 0,$$

and is therefore invertible. Also, the binary operation specified for $M$ is the same as the binary operation of GL(2). We show that the three subgroup properties hold for $M$.

**SG1** Let $\mathbf{A}, \mathbf{B} \in M$. Then

$$\mathbf{A} = \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} v & w \\ 0 & v \end{pmatrix},$$

for some $r, s, v, w \in \mathbb{R}$ with $r \neq 0$ and $v \neq 0$. So

$$\mathbf{AB} = \begin{pmatrix} r & s \\ 0 & r \end{pmatrix} \begin{pmatrix} v & w \\ 0 & v \end{pmatrix} = \begin{pmatrix} rv & rw + sv \\ 0 & rv \end{pmatrix}.$$

This matrix is of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a = rv$ and $b = rw + sv$. Also, $rv \neq 0$ since $r \neq 0$ and $v \neq 0$. Hence $\mathbf{AB} \in M$. Thus $M$ is closed under matrix multiplication.

**SG2** The identity element

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of GL(2) is of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a = 1$ and $b = 0$. So $\mathbf{I} \in M$.

**SG3** Let $\mathbf{A} \in M$. Then

$$\mathbf{A} = \begin{pmatrix} r & s \\ 0 & r \end{pmatrix},$$

for some $r, s \in \mathbb{R}$ with $r \neq 0$. The inverse of $\mathbf{A}$ in GL(2) is

$$\mathbf{A}^{-1} = \frac{1}{r^2} \begin{pmatrix} r & -s \\ 0 & r \end{pmatrix} = \begin{pmatrix} 1/r & -s/r^2 \\ 0 & 1/r \end{pmatrix}.$$

This matrix is of the form

$$\begin{pmatrix} a & b \\ 0 & a \end{pmatrix}$$

with $a = 1/r$ and $b = -s/r^2$. Also $1/r \neq 0$. Hence $\mathbf{A}^{-1} \in M$. Thus $M$ contains the inverse of each of its elements.

Since the three subgroup properties hold, $M$ is a subgroup of GL(2). Hence it is a group under matrix multiplication.

**(b)** The set $P$ is a subset of the group GL(2), because each matrix

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$$

in $P$ has determinant

$$a \times \frac{1}{a} - 0 \times 0 = 1,$$

and is therefore invertible. Also, the binary operation specified for $P$ is the same as the binary operation of GL(2). We show that the three subgroup properties hold for $P$.

**SG1** Let $\mathbf{A}, \mathbf{B} \in P$. Then

$$\mathbf{A} = \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} \quad \text{and} \quad \mathbf{B} = \begin{pmatrix} y & 0 \\ 0 & 1/y \end{pmatrix},$$

for some $x, y \in \mathbb{R}$ with $x \neq 0$ and $y \neq 0$. So

$$\mathbf{AB} = \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix} \begin{pmatrix} y & 0 \\ 0 & 1/y \end{pmatrix} = \begin{pmatrix} xy & 0 \\ 0 & 1/(xy) \end{pmatrix}.$$

This matrix is of the form

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$$

with $a = xy$. Also, $xy \neq 0$ since $x \neq 0$ and $y \neq 0$. Hence $\mathbf{AB} \in P$. Thus $P$ is closed under matrix multiplication.

**SG2** The identity element

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

of GL(2) is in $P$, since we can write

$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1/1 \end{pmatrix},$$

which shows that $\mathbf{I}$ is of the form

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$$

with $a = 1$.

**SG3** Let $\mathbf{A} \in P$. Then

$$\mathbf{A} = \begin{pmatrix} x & 0 \\ 0 & 1/x \end{pmatrix},$$

for some $x \in \mathbb{R}$ with $x \neq 0$. The inverse of $\mathbf{A}$ in GL(2) is

$$\mathbf{A}^{-1} = \frac{1}{1} \begin{pmatrix} 1/x & 0 \\ 0 & x \end{pmatrix},$$

which we can write as

$$\mathbf{A}^{-1} = \begin{pmatrix} 1/x & 0 \\ 0 & 1/(1/x) \end{pmatrix}.$$

This matrix is of the form

$$\begin{pmatrix} a & 0 \\ 0 & 1/a \end{pmatrix}$$

with $a = 1/x$. Also, $1/x \neq 0$. Hence $\mathbf{A}^{-1} \in P$. Thus $P$ contains the inverse of each of its elements.

Since the three subgroup properties hold, $P$ is a subgroup of GL(2). Hence it is a group under matrix multiplication.

(Another way to show that this set $P$ is a subgroup of GL(2) is to use Theorem B81 from Unit B4, which states that the intersection of two subgroups of a group is always a subgroup of the group.

The set $P$ can be written as

$$P = \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} : a, d \in \mathbb{R},\ ad = 1 \right\}.$$

So it is the set of all matrices in GL(2) that are diagonal and have determinant 1. Hence it is the intersection of $D$, the set of diagonal matrices in GL(2), and SL(2), the set of matrices in GL(2) with determinant 1. Each of these sets is a subgroup of GL(2), by the results of Exercises E19 and E20 respectively, so it follows from Theorem B81 that $P$ is also a subgroup of GL(2).)

## Solution to Exercise E22

Consider, for example, the matrix

$$\mathbf{A} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}.$$

This matrix is in $X$, because it is of the form

$$\begin{pmatrix} a & b \\ c & 1 \end{pmatrix}$$

with $a = 2$ and $b = c = 1$, and

$$a - bc = 2 - 1 \times 1 = 1 \neq 0.$$

However,

$$\mathbf{A}^2 = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix},$$

and this matrix is not in $X$, because it is not of the form

$$\begin{pmatrix} a & b \\ c & 1 \end{pmatrix},$$

as its bottom right entry is not 1. Thus $X$ is not closed under matrix multiplication.

Hence property SG1 fails, so $X$ is not a subgroup of GL(2).

## Solution to Exercise E23

**(a)** $x^3 \circ x = x^4$ translates to

$$3x + x = 4x.$$

**(b)** $x^5 \circ x^{-5} = e$ translates to

$$5x + (-5)x = 0.$$

**(c)** $(x^4)^{-1} = (x^{-1})^4$ translates to

$$-(4x) = 4(-x).$$

## Solution to Exercise E24

**(a)** **(i)** In $S(\square)$,

$$a^2 = a \circ a = b,$$
$$a^3 = a^2 \circ a = b \circ a = c,$$
$$a^4 = a^3 \circ a = c \circ a = e.$$

Thus $a$ has order 4.

**(ii)** In $S(\square)$, $b^2 = e$, so $b$ has order 2.

**(iii)** In $S(\square)$, $r^2 = e$, so $r$ has order 2.

**(b)** The identity element of $(U_9, \times_9)$ is 1.

**(i)** The consecutive powers of 5 in $(U_9, \times_9)$ starting from $5^1$ are

$$5^1, 5^2, 5^3, 5^4, 5^5, 5^6, \ldots,$$

that is,

$$5, 7, 8, 4, 2, 1, \ldots.$$

So 5 has order 6 in $(U_9, \times_9)$.

(The first power in the list equal to 1 is the sixth power.)

**(ii)** The consecutive powers of 2 in $(U_9, \times_9)$ starting from $2^1$ are

$$2, 4, 8, 7, 5, 1, \ldots.$$

So 2 has order 6 in $(U_9, \times_9)$.

(Alternatively, the list of consecutive powers of 5 in part (b)(i) shows that $5^{-1} = 2$ in $(U_9, \times_9)$. Hence the order of 2 is the same as the order of 5, so the order of 2 is 6.

To see why the list of consecutive powers of 5 shows that $5^{-1} = 2$ in $(U_9, \times_9)$, use the fact that each integer in the list is obtained by composing the previous integer with 5 in $(U_9, \times_9)$. The integer 1 appears immediately after the integer 2 in the list, so $2 \times_9 5 = 1$ and hence $5^{-1} = 2$.)

**(iii)** The consecutive powers of 7 in $(U_9, \times_9)$ starting from $7^1$ are

$$7, 4, 1, \ldots.$$

So 7 has order 3 in $(U_9, \times_9)$.

(The list of consecutive powers of 7 in $(U_9, \times_9)$ can be obtained simply by working them out, or alternatively by using the list of powers of 5 in part (b)(i). If we start at $5^2 = 7$ in the list of powers of 5 and go forward two places at a time, then we obtain the powers

$$5^2, 5^4, 5^6, 5^8, \ldots,$$

that is,

$$5^2, (5^2)^2, (5^2)^3, (5^2)^4, \ldots.$$

Hence we obtain the list of powers of $5^2 = 7$.)

**(c)** The group $(\mathbb{Z}_8, +_8)$ is additive, so the order of an element $x$ in this group is the *smallest* positive integer $n$ such that the *multiple* $nx$ is equal to the identity element, 0.

**(i)** The consecutive multiples of 2 in $(\mathbb{Z}_8, +_8)$ starting from 1(2) are

$$1(2),\ 2(2),\ 3(2),\ 4(2),\ \ldots,$$

that is,

$$2, 4, 6, 0, \ldots.$$

So 2 has order 4 in $(\mathbb{Z}_8, +_8)$.

(The first multiple in the list equal to 0 is the 4th multiple.)

(To calculate the consecutive multiples of 2 in $(\mathbb{Z}_8, +_8)$, we calculate

$$2(2) = 2 +_8 2 = 4,$$
$$3(2) = 2 +_8 2 +_8 2 = 6,$$
$$4(2) = 2 +_8 2 +_8 2 +_8 2 = 0,$$

and so on.

That is, we start with 2 and successively add 2 modulo 8 to each multiple to obtain the next multiple.)

**(ii)** The consecutive multiples of 3 in $(\mathbb{Z}_8, +_8)$ starting from 1(3) are

$$3, 6, 1, 4, 7, 2, 5, 0, \ldots.$$

So 3 has order 8 in $(\mathbb{Z}_8, +_8)$.

**(iii)** The consecutive multiples of 6 in $(\mathbb{Z}_8, +_8)$ starting from 1(6) are

$$6, 4, 2, 0, \ldots.$$

So 6 has order 4 in $(\mathbb{Z}_8, +_8)$.

(The fact that 6 has order 4 also follows from part (c)(i), since 6 is the inverse of 2 in $(\mathbb{Z}_8, +_8)$ and hence has the same order as 2.)

(An alternative way to find the orders of elements in a group $(\mathbb{Z}_n, +_n)$ is to use Theorem B38 from Unit B2, which you will revise in the next subsection.)

## Solution to Exercise E25

The identity element of GL(2) is $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

**(a)** In GL(2),

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^3 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix},$$

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^4 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ has order 4.

**(b)** The matrix $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ is the identity element of GL(2), so it has order 1.

**(c)** In GL(2),

$$\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Thus $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ has order 2.

**(d)** In GL(2),

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^2 = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^3 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix},$$

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^4 = \begin{pmatrix} 1 & 3 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 4 \\ 0 & 1 \end{pmatrix}.$$

This pattern will continue because for any positive integer $k$ we have

$$\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}.$$

Hence in general for any positive integer $n$ we have

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}.$$

(This can be proved formally by using mathematical induction.)

Thus there is no positive integer $n$ such that

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^n = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Hence $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ has infinite order.

## Solution to Exercise E26

**(a)** The permutation (2 3)(6 9 8) has order 6.

**(b)** The permutation (1 7 3 2 4) has order 5.

**(c)** The permutation (1 7)(3 6 4 5) has order 4.

## Solution to Exercise E27

In each case, the order of the cyclic subgroup is equal to the order of the group element that generates it. You found this order in Exercise E24, and in the same exercise you also worked out consecutive powers (or multiples) of this element, which give all the elements of the cyclic subgroup.

**(a)** The required cyclic subgroups of $S(\square)$ are as follows.

**(i)** $\langle a \rangle = \{e, a, b, c\}$
**(ii)** $\langle b \rangle = \{e, b\}$
**(iii)** $\langle r \rangle = \{e, r\}$

(The consecutive powers of $a$, $b$ and $r$ in $S(\square)$ are:

$$\ldots, e, a, b, c, e, a, b, c, \ldots,$$
$$\ldots, e, b, e, b, e, b, \ldots,$$
$$\ldots, e, r, e, r, e, r, \ldots.)$$

**(b)** The required cyclic subgroups of $(U_9, \times_9)$ are as follows.

**(i)** $\langle 5 \rangle = \{1, 5, 7, 8, 4, 2\}$
**(ii)** $\langle 2 \rangle = \{1, 2, 4, 8, 7, 5\}$ (Thus $\langle 2 \rangle = \langle 5 \rangle$.)
**(iii)** $\langle 7 \rangle = \{1, 7, 4\}$

(The consecutive powers of 5, 2 and 7 in $(U_9, \times_9)$ are:

$$\ldots, 1, 5, 7, 8, 4, 2, 1, 5, 7, 8, 4, 2, \ldots,$$
$$\ldots, 1, 2, 4, 8, 7, 5, 1, 2, 4, 8, 7, 5, \ldots,$$
$$\ldots, 1, 7, 4, 1, 7, 4, \ldots.)$$

**(c)** The required cyclic subgroups of $(\mathbb{Z}_8, +_8)$ are as follows.

**(i)** $\langle 2\rangle = \{0, 2, 4, 6\}$

**(ii)** $\langle 3\rangle = \{0, 3, 6, 1, 4, 7, 2, 5\}$ (Thus $\langle 3\rangle = \mathbb{Z}_8$.)

**(iii)** $\langle 6\rangle = \{0, 6, 4, 2\}$ (Thus $\langle 6\rangle = \langle 2\rangle$.)

(The consecutive multiples of 2, 3 and 6 in $(\mathbb{Z}_8, +_8)$ are:

$\ldots, 0, 2, 4, 6, 0, 2, 4, 6, \ldots,$
$\ldots, 0, 3, 6, 1, 4, 7, 2, 5, 0, 3, 6, 1, 4, 7, 2, 5, \ldots,$
$\ldots, 0, 6, 4, 2, 0, 6, 4, 2, \ldots.)$

## Solution to Exercise E28

**(a)** In $S(\square)$,

$\langle e\rangle = \{e\},$
$\langle a\rangle = \{e, a, b, c\} = \langle c\rangle$ (since $c = a^{-1}$),
$\langle b\rangle = \{e, b\},$
$\langle r\rangle = \{e, r\},$
$\langle s\rangle = \{e, s\},$
$\langle t\rangle = \{e, t\},$
$\langle u\rangle = \{e, u\}.$

Thus $S(\square)$ has seven distinct cyclic subgroups:

$\{e\}, \quad \{e, a, b, c\},$
$\{e, b\}, \quad \{e, r\}, \quad \{e, s\}, \quad \{e, t\}, \quad \{e, u\}.$

(As well as these seven cyclic subgroups, $S(\square)$ has three further subgroups, which are non-cyclic. These are $S(\square)$ itself, and two subgroups of order 4, namely $\{e, b, r, t\}$ and $\{e, b, s, u\}$. The two non-cyclic subgroups of order 4 can be obtained by modifying the square, as given in the solution to Exercise E15(c).)

**(b)** In the additive group $(\mathbb{Z}_9, +_9)$,

$\langle 0\rangle = \{0\},$
$\langle 1\rangle = \{0, 1, 2, 3, 4, 5, 6, 7, 8\} = \mathbb{Z}_9 = \langle 8\rangle,$
(since 8 is the inverse of 1),
$\langle 2\rangle = \{0, 2, 4, 6, 8, 1, 3, 5, 7\} = \mathbb{Z}_9 = \langle 7\rangle,$
(since 7 is the inverse of 2),
$\langle 3\rangle = \{0, 3, 6\} = \langle 6\rangle,$
(since 6 is the inverse of 3),
$\langle 4\rangle = \{0, 4, 8, 3, 7, 2, 6, 1, 5\} = \mathbb{Z}_9 = \langle 5\rangle,$
(since 5 is the inverse of 4).

Thus $(\mathbb{Z}_9, +_9)$ has three distinct cyclic subgroups:

$\{0\}, \quad \{0, 3, 6\}, \quad \mathbb{Z}_9.$

**(c)** In $(\mathbb{Z}_7^*, \times_7)$, we have $2 \times_7 4 = 1$, so 2 and 4 are inverses of each other, and $3 \times_7 5 = 1$, so 3 and 5 are inverses of each other.

In $(\mathbb{Z}_7^*, \times_7)$,

$\langle 1\rangle = \{1\},$
$\langle 2\rangle = \{1, 2, 4\} = \langle 4\rangle$ (since $4 = 2^{-1}$),
$\langle 3\rangle = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_7^* = \langle 5\rangle$ (since $5 = 3^{-1}$),
$\langle 6\rangle = \{1, 6\}.$

Thus $(\mathbb{Z}_7^*, \times_7)$ has four distinct cyclic subgroups:

$\{1\}, \quad \{1, 6\}, \quad \{1, 2, 4\}, \quad \mathbb{Z}_7^*.$

**(d)** In $S_3$,

$\langle e\rangle = \{e\},$
$\langle (1\ 2)\rangle = \{e, (1\ 2)\},$
$\langle (1\ 3)\rangle = \{e, (1\ 3)\},$
$\langle (2\ 3)\rangle = \{e, (2\ 3)\},$
$\langle (1\ 2\ 3)\rangle = \{e, (1\ 2\ 3), (1\ 3\ 2)\} = \langle (1\ 3\ 2)\rangle$
(since $(1\ 2\ 3)^{-1} = (1\ 3\ 2)$).

Thus $S_3$ has five distinct cyclic subgroups:

$\{e\}, \quad \{e, (1\ 2)\}, \quad \{e, (1\ 3)\}, \quad \{e, (2\ 3)\},$
$\{e, (1\ 2\ 3), (1\ 3\ 2)\}.$

## Solution to Exercise E29

**(a)** The group $S(\square)$ is non-cyclic because it has order 8 but contains no element of order 8:

the identity element has order 1,
the four reflections have order 2,
the rotation $b$ has order 2,
the rotations $a$ and $c$ have order 4.

**(b)** The group $S^+(\square)$ is cyclic because it has order 4 and contains two elements ($a$ and $c$) of order 4; each of these elements is a generator of the group.

**(c)** The group $(\mathbb{Z}_5, +_5)$ is cyclic because it has order 5 and contains four elements (1, 2, 3 and 4) of order 5; each of these elements is a generator of the group.

**(d)** We have

$$U_8 = \{1, 3, 5, 7\}.$$

We find the orders of the elements of $(U_8, \times_8)$.

The identity element 1 has order 1.

The consecutive powers of 3 are

$$\ldots, 1, 3, 1, 3, \ldots,$$

so 3 has order 2.

The consecutive powers of 5 are

$$\ldots, 1, 5, 1, 5, \ldots,$$

so 5 has order 2.

The consecutive powers of 7 are

$$\ldots, 1, 7, 1, 7, \ldots,$$

so 7 has order 2.

Thus $(U_8, \times_8)$ has order 4 but contains no element of order 4, so it is non-cyclic.

## Solution to Exercise E30

**(a)** By Theorem B38, the orders of the elements of $(\mathbb{Z}_{14}, +_{14})$ are as follows.

| Element | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Order | 1 | 14 | 7 | 14 | 7 | 14 | 7 | 2 | 7 | 14 | 7 | 14 | 7 | 14 |

**(b)** By Corollary B40, or by the answers to part (a), the generators of $(\mathbb{Z}_{14}, +_{14})$ are 1, 3, 5, 9, 11 and 13.

## Solution to Exercise E31

By Theorem B41, $(\mathbb{Z}_{16}, +_{16})$ has five subgroups, with orders 1, 2, 4, 8 and 16 (the factors of 16). They are:

$$\begin{aligned}
\langle 0 \rangle &= \{0\},\\
\langle 8 \rangle &= \{0, 8\},\\
\langle 4 \rangle &= \{0, 4, 8, 12\},\\
\langle 2 \rangle &= \{0, 2, 4, 6, 8, 10, 12, 14\},\\
\langle 1 \rangle &= \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10,\\
&\qquad\qquad 11, 12, 13, 14, 15\} = \mathbb{Z}_{16}.
\end{aligned}$$

## Solution to Exercise E32

**(a)** $U_{10} = \{1, 3, 7, 9\}$.

**(b)**

| $\times_{10}$ | 1 | 3 | 7 | 9 |
|---|---|---|---|---|
| 1 | 1 | 3 | 7 | 9 |
| 3 | 3 | 9 | 1 | 7 |
| 7 | 7 | 1 | 9 | 3 |
| 9 | 9 | 7 | 3 | 1 |

**(c)** The group table found in part (b) can be rearranged as follows:

| $\times_{10}$ | 1 | 3 | 9 | 7 |
|---|---|---|---|---|
| 1 | 1 | 3 | 9 | 7 |
| 3 | 3 | 9 | 7 | 1 |
| 9 | 9 | 7 | 1 | 3 |
| 7 | 7 | 1 | 3 | 9 |

This has the same pattern as the group table of $(\mathbb{Z}_4, +_4)$, which is

| $+_4$ | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | 3 | 0 |
| 2 | 2 | 3 | 0 | 1 |
| 3 | 3 | 0 | 1 | 2 |

An isomorphism from $(U_{10}, \times_{10})$ to $(\mathbb{Z}_4, +_4)$ is

$$\begin{aligned}
\phi : U_{10} &\longrightarrow \mathbb{Z}_4\\
1 &\longmapsto 0\\
3 &\longmapsto 1\\
9 &\longmapsto 2\\
7 &\longmapsto 3.
\end{aligned}$$

(The group table found in part (b) can also be rearranged as follows.

| $\times_{10}$ | 1 | 7 | 9 | 3 |
|---|---|---|---|---|
| 1 | 1 | 7 | 9 | 3 |
| 7 | 7 | 9 | 3 | 1 |
| 9 | 9 | 3 | 1 | 7 |
| 3 | 3 | 1 | 7 | 9 |

This gives the following alternative isomorphism from $(U_{10}, \times_{10})$ to $(\mathbb{Z}_4, +_4)$:

$$\begin{aligned}
\phi : U_{10} &\longrightarrow \mathbb{Z}_4\\
1 &\longmapsto 0\\
7 &\longmapsto 1\\
9 &\longmapsto 2\\
3 &\longmapsto 3.)
\end{aligned}$$

## Solution to Exercise E33

Let $\phi$ be the mapping

$$\begin{aligned}\phi : \mathbb{Z} &\longrightarrow 3\mathbb{Z}\\ n &\longmapsto 3n,\end{aligned}$$

as given in the question.

Then $\phi$ is one-to-one, because if $m$ and $n$ are elements of $\mathbb{Z}$ such that $\phi(m) = \phi(n)$, then $3m = 3n$ and hence $m = n$.

Also, $\phi$ is onto, because any element of $3\mathbb{Z}$ is of the form $3n$ where $n \in \mathbb{Z}$, and this element is the image under $\phi$ of the element $n$ of $\mathbb{Z}$.

Finally, if $m, n \in \mathbb{Z}$, then

$$\begin{aligned}\phi(m+n) &= 3(m+n)\\ &= 3m + 3n\\ &= \phi(m) + \phi(n).\end{aligned}$$

Thus $\phi$ is an isomorphism and hence $(\mathbb{Z}, +) \cong (3\mathbb{Z}, +)$.

## Solution to Exercise E34

The group $(G, \times)$ from Exercise E3 is a group of order 4 all of whose elements are self-inverse. Therefore it is isomorphic to the Klein four-group $V$ (and $S(\square)$).

## Solution to Exercise E35

We have

$$U_{18} = \{1, 5, 7, 11, 13, 17\}.$$

Thus $U_{18}$ is a group of order 6. It is abelian, since $\times_{18}$ is a commutative binary operation. Therefore it is isomorphic to $\mathbb{Z}_6$ (and $C_6$).

## Solution to Exercise E36

**(a)** The left cosets of $\{e, s\}$ in $S(\triangle)$ are

$$\begin{aligned}eH &= \{e \circ e, e \circ s\} = \{e, s\} = H,\\ aH &= \{a \circ e, a \circ s\} = \{a, r\},\\ bH &= \{b \circ e, b \circ s\} = \{b, t\},\\ rH &= \{r \circ e, r \circ s\} = \{r, a\},\\ sH &= \{s \circ e, s \circ s\} = \{s, e\} = H,\\ tH &= \{t \circ e, t \circ s\} = \{t, b\}.\end{aligned}$$

**(b)** The distinct left cosets of $H = \{e, s\}$ in $S(\triangle)$ are

$$\{e, s\}, \quad \{a, r\}, \quad \{b, t\}.$$

## Solution to Exercise E37

**(a)** The consecutive powers of 2 in $\mathbb{Z}_7^*$ starting from $2^1$ are

$$2, 4, 1, \ldots.$$

Thus $\langle 2 \rangle = \{1, 2, 4\}$. That is, $H = \{1, 2, 4\}$ is the cyclic subgroup of $\mathbb{Z}_7^*$ generated by 2.

**(b)** The left cosets of $H = \{1, 2, 4\}$ in $\mathbb{Z}_7^*$ are

$$\begin{aligned}1H &= \{1 \times_7 1,\ 1 \times_7 2,\ 1 \times_7 4\} = \{1, 2, 4\} = H,\\ 2H &= \{2 \times_7 1,\ 2 \times_7 2,\ 2 \times_7 4\} = \{2, 4, 1\} = H,\\ 3H &= \{3 \times_7 1,\ 3 \times_7 2,\ 3 \times_7 4\} = \{3, 6, 5\},\\ 4H &= \{4 \times_7 1,\ 4 \times_7 2,\ 4 \times_7 4\} = \{4, 1, 2\} = H,\\ 5H &= \{5 \times_7 1,\ 5 \times_7 2,\ 5 \times_7 4\} = \{5, 3, 6\},\\ 6H &= \{6 \times_7 1,\ 6 \times_7 2,\ 6 \times_7 4\} = \{6, 5, 3\}.\end{aligned}$$

**(c)** The distinct left cosets of $H = \{1, 2, 4\}$ in $\mathbb{Z}_7^*$ are

$$\{1, 2, 4\}, \quad \{3, 5, 6\}.$$

## Solution to Exercise E38

**(a)** The subgroup $H = \{e, a, b, c\}$ is one left coset, by Proposition E3(b).

All the left cosets of $H$ contain the same number of elements as $H$ by Proposition E3(d), and distinct left cosets are disjoint from each other by Proposition E3(c).

It follows that there is just one other left coset, namely $\{r, s, t, u\}$.

So the distinct left cosets of $H$ in $S(\square)$ are

$$\{e, a, b, c\}, \quad \{r, s, t, u\}.$$

**(b)** All the left cosets of $H$ contain the same number of elements by Proposition E3(d).

Thus each left coset of the subgroup $H = \{e\}$ has just one element.

Hence there are eight distinct left cosets of $H$ in $S(\square)$, each with one element:

$$\{e\},\ \{a\},\ \{b\},\ \{c\},\ \{r\},\ \{s\},\ \{t\},\ \{u\}.$$

**(c)** The subgroup $S(\square)$ is the whole group, and so is the only left coset by Proposition E3(b) and (c).

## Solution to Exercise E39

We have

$$U_{20} = \{1, 3, 7, 9, 11, 13, 17, 19\}.$$

Also,

$$19 \times 19 \equiv (-1) \times (-1) \equiv 1 \pmod{20},$$

so

$$19 \times_{20} 19 = 1.$$

Hence $\langle 19 \rangle = \{1, 19\}$, so $H = \{1, 19\}$ is the cyclic subgroup of $U_{20}$ generated by 19.

By Strategy E1, the left cosets of $H = \{1, 19\}$ in $U_{20}$ are

$$\begin{aligned} H &= \{1, 19\}, \\ 3H &= \{3 \times_{20} 1, 3 \times_{20} 19\} = \{3, 17\}, \\ 7H &= \{7 \times_{20} 1, 7 \times_{20} 19\} = \{7, 13\}, \\ 9H &= \{9 \times_{20} 1, 9 \times_{20} 19\} = \{9, 11\}. \end{aligned}$$

The partition of $U_{20}$ into left cosets of $H$ is therefore

$$\{1, 19\}, \quad \{3, 17\}, \quad \{7, 13\}, \quad \{9, 11\}.$$

(A quick way of obtaining the second element in each of the left cosets above is as follows:

$$\begin{aligned} &3 \times 19 \equiv 3 \times (-1) \equiv -3 \equiv 17 \pmod{20}, \\ &7 \times 19 \equiv 7 \times (-1) \equiv -7 \equiv 13 \pmod{20}, \\ &9 \times 19 \equiv 9 \times (-1) \equiv -9 \equiv 11 \pmod{20}.) \end{aligned}$$

## Solution to Exercise E40

By Strategy E1, the left cosets of $H = \{e, t\}$ in $S(\triangle)$ are

$$\begin{aligned} H &= \{e, t\}, \\ aH &= \{a \circ e, a \circ t\} = \{a, s\}, \\ bH &= \{b \circ e, b \circ t\} = \{b, r\}. \end{aligned}$$

The partition of $S(\triangle)$ into left cosets of $H$ is therefore

$$\{e, t\}, \quad \{a, s\}, \quad \{b, r\}.$$

## Solution to Exercise E41

Using Strategy E1, we find that the left cosets of $H$ in $A_4$ are

$$H = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

$$\begin{aligned} &(1\ 2\ 3)H \\ &= \{(1\ 2\ 3) \circ e,\ (1\ 2\ 3) \circ (1\ 2)(3\ 4), \\ &\quad (1\ 2\ 3) \circ (1\ 3)(2\ 4),\ (1\ 2\ 3) \circ (1\ 4)(2\ 3)\} \\ &= \{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\}, \end{aligned}$$

$$\begin{aligned} &(1\ 3\ 2)H \\ &= \{(1\ 3\ 2) \circ e,\ (1\ 3\ 2) \circ (1\ 2)(3\ 4), \\ &\quad (1\ 3\ 2) \circ (1\ 3)(2\ 4), (1\ 3\ 2) \circ (1\ 4)(2\ 3)\} \\ &= \{(1\ 3\ 2), (2\ 3\ 4), (1\ 2\ 4), (1\ 4\ 3)\}. \end{aligned}$$

In summary, the partition into left cosets is

$$\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\},$$

$$\{(1\ 2\ 3), (1\ 3\ 4), (2\ 4\ 3), (1\ 4\ 2)\},$$

$$\{(1\ 3\ 2), (2\ 3\ 4), (1\ 2\ 4), (1\ 4\ 3)\}.$$

## Solution to Exercise E42

The right cosets of $H = \{e, s\}$ in $S(\triangle)$ are

$$\begin{aligned} H &= \{e, s\}, \\ Ha &= \{e \circ a, s \circ a\} = \{a, t\}, \\ Hb &= \{e \circ b, s \circ b\} = \{b, r\}. \end{aligned}$$

The partition of $S(\triangle)$ into right cosets of $H$ is therefore

$$\{e, s\}, \quad \{a, t\}, \quad \{b, r\}.$$

## Solution to Exercise E43

**$\Longrightarrow$ part**

Suppose that

$$x \in yH.$$

Then

$$x = yh$$

for some $h \in H$. Composing each side of this equation with $x^{-1}$ on the right gives

$$xx^{-1} = yhx^{-1},$$

that is,

$$e = yhx^{-1}.$$

Now composing each side of this equation with $y^{-1}$ on the left gives

$$y^{-1}e = y^{-1}yhx^{-1},$$

that is,

$$y^{-1} = hx^{-1}.$$

Hence $y^{-1} \in Hx^{-1}$, as required.

**$\Longleftarrow$ part**

Now suppose that

$$y^{-1} \in Hx^{-1}.$$

Then

$$y^{-1} = hx^{-1}$$

for some $h \in H$. Composing each side of this equation with $x$ on the right gives

$$y^{-1}x = hx^{-1}x,$$

that is,

$$y^{-1}x = h.$$

Now composing each side of this equation with $y$ on the left gives

$$yy^{-1}x = yh,$$

that is,

$$x = yh.$$

Hence $x \in yH$, as required.

This completes the proof.

## Solution to Exercise E44

**(a)** Using Strategy E1, we find that the cosets are

$$\begin{aligned} H &= \{0, 2, 4, 6, 8\}, \\ 1 + H &= 1 + \{0, 2, 4, 6, 8\} \\ &= \{1 +_{10} 0,\ 1 +_{10} 2,\ 1 +_{10} 4,\ 1 +_{10} 6,\ 1 +_{10} 8\} \\ &= \{1, 3, 5, 7, 9\}. \end{aligned}$$

In summary, the partition is

$$\{0, 2, 4, 6, 8\}, \quad \{1, 3, 5, 7, 9\}.$$

(In fact, there is no need to work out the second coset in the way above, because the group $\mathbb{Z}_{10}$ and the subgroup $H$ have orders 10 and 5, respectively, so there are two cosets each containing 5 elements, and hence the second coset contains all the elements of $\mathbb{Z}_{10}$ that are not in the first coset $H$.)

**(b)** Using Strategy E1, we find that the cosets are

$$\begin{aligned} H &= \{0, 5\}, \\ 1 + H &= 1 + \{0, 5\} \\ &= \{1 +_{10} 0,\ 1 +_{10} 5\} \\ &= \{1, 6\}, \\ 2 + H &= 2 + \{0, 5\} \\ &= \{2 +_{10} 0,\ 2 +_{10} 5\} \\ &= \{2, 7\}, \\ 3 + H &= 3 + \{0, 5\} \\ &= \{3 +_{10} 0,\ 3 +_{10} 5\} \\ &= \{3, 8\}, \\ 4 + H &= 4 + \{0, 5\} \\ &= \{4 +_{10} 0,\ 4 +_{10} 5\} \\ &= \{4, 9\}. \end{aligned}$$

In summary, the partition is

$$\{0, 5\}, \quad \{1, 6\}, \quad \{2, 7\}, \quad \{3, 8\}, \quad \{4, 9\}.$$

(Similarly to part (a), there is no need to work out the final coset in the way above, as it must contain the two elements of $\mathbb{Z}_{10}$ not yet assigned to a coset. However, working out the final coset is a useful check.)

## Solution to Exercise E45

**(a)** The cosets of $4\mathbb{Z}$ in $\mathbb{Z}$ are

$$\begin{aligned} 4\mathbb{Z} &= \{\ldots, -8, -4, 0, 4, 8, \ldots\}, \\ 1 + 4\mathbb{Z} &= \{\ldots, -7, -3, 1, 5, 9, \ldots\}, \\ 2 + 4\mathbb{Z} &= \{\ldots, -6, -2, 2, 6, 10, \ldots\}, \\ 3 + 4\mathbb{Z} &= \{\ldots, -5, -1, 3, 7, 11, \ldots\}. \end{aligned}$$

**(b)** The cosets of $6\mathbb{Z}$ in $2\mathbb{Z}$ are

$$\begin{aligned} 6\mathbb{Z} &= \{\ldots, -12, -6, 0, 6, 12, \ldots\}, \\ 2 + 6\mathbb{Z} &= \{\ldots, -10, -4, 2, 8, 14, \ldots\}, \\ 4 + 6\mathbb{Z} &= \{\ldots, -8, -2, 4, 10, 16, \ldots\}. \end{aligned}$$

(Here the whole group $2\mathbb{Z}$ consists of only the *even* integers, so there are no cosets such as $1 + 6\mathbb{Z}$.)

## Solution to Exercise E46

**(a)** By Exercise E40, the partition of $S(\triangle)$ into left cosets of the subgroup $\{e, t\}$ is

$$\{e, t\}, \quad \{a, s\}, \quad \{b, r\}.$$

In $S(\triangle)$ the elements $a$ and $b$ are inverses of each other and all the other elements are self-inverse. So the partition of $S(\triangle)$ into right cosets of the subgroup $\{e, t\}$ is

$$\{e, t\}, \quad \{b, s\}, \quad \{a, r\},$$

that is,

$$\{e, t\}, \quad \{a, r\}, \quad \{b, s\}.$$

Since the two partitions are different, $\{e, t\}$ is not a normal subgroup of $S(\triangle)$.

**(b)** All the left cosets of the subgroup $S^+(\triangle) = \{e, a, b\}$ in $S(\triangle)$ contain three elements and one of the left cosets is the subgroup itself, and the same is true for the right cosets. So the partition of $S(\triangle)$ into left cosets of $\{e, a, b\}$ and the partition of $S(\triangle)$ into right cosets of $\{e, a, b\}$ are both

$$\{e, a, b\}, \quad \{r, s, t\}.$$

Since the two partitions are the same, $S^+(\triangle) = \{e, a, b\}$ is a normal subgroup of $S(\triangle)$.

**(c)** Every left coset and every right coset of the subgroup $\{e\}$ in $S(\triangle)$ contains just one element, so the partition of $S(\triangle)$ into left cosets of $\{e\}$ and the partition of $S(\triangle)$ into right cosets of $\{e\}$ are both

$$\{e\}, \ \{a\}, \ \{b\}, \ \{r\}, \ \{s\}, \ \{t\}.$$

Since the two partitions are the same, $\{e\}$ is a normal subgroup of $S(\triangle)$.

**(d)** The only left coset and the only right coset of $S(\triangle)$ in $S(\triangle)$ is $S(\triangle)$.

So the partition into left cosets and the partition into right cosets are both simply $S(\triangle)$.

Since the two partitions are the same, $S(\triangle)$ is a normal subgroup of $S(\triangle)$.

## Solution to Exercise E47

**(a)** The left coset $(1\ 2)(3\ 4)H$ is

$$\begin{aligned}&(1\ 2)(3\ 4)H\\ &= \{(1\ 2)(3\ 4) \circ e,\ (1\ 2)(3\ 4) \circ (1\ 2\ 3),\\ &\qquad (1\ 2)(3\ 4) \circ (1\ 3\ 2)\}\\ &= \{(1\ 2)(3\ 4),\ (2\ 4\ 3),\ (1\ 4\ 3)\}.\end{aligned}$$

The right coset $H(1\ 2)(3\ 4)$ is

$$\begin{aligned}&H(1\ 2)(3\ 4)\\ &= \{e \circ (1\ 2)(3\ 4),\ (1\ 2\ 3) \circ (1\ 2)(3\ 4),\\ &\qquad (1\ 3\ 2) \circ (1\ 2)(3\ 4)\}\\ &= \{(1\ 2)(3\ 4),\ (1\ 3\ 4),\ (2\ 3\ 4)\}.\end{aligned}$$

So the left coset $(1\ 2)(3\ 4)H$ and the right coset $H(1\ 2)(3\ 4)$ are not the same. Since the permutation $(1\ 2)(3\ 4)$ lies in both these cosets, the partition of $A_4$ into left cosets of $H$ is not the same as its partition into right cosets of $H$. Hence $H$ is not a normal subgroup of $A_4$.

**(b)** By the solution to Exercise E41, the left cosets of $K$ in $A_4$ are

$$\{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\},$$
$$\{(1\ 2\ 3),\ (1\ 3\ 4),\ (2\ 4\ 3),\ (1\ 4\ 2)\},$$
$$\{(1\ 3\ 2),\ (2\ 3\ 4),\ (1\ 2\ 4),\ (1\ 4\ 3)\}.$$

By replacing each permutation by its inverse, we find that the right cosets of $K$ in $A_4$ are

$$\{e,\ (1\ 2)(3\ 4),\ (1\ 3)(2\ 4),\ (1\ 4)(2\ 3)\},$$
$$\{(1\ 3\ 2),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (1\ 2\ 4)\},$$
$$\{(1\ 2\ 3),\ (2\ 4\ 3),\ (1\ 4\ 2),\ (1\ 3\ 4)\}.$$

These are the same sets as in the partition into left cosets (just in a different order and with their elements listed in a different order). So the partition of $A_4$ into left cosets of $K$ and the partition of $A_4$ into right cosets of $K$ are the same. Hence $K$ is a normal subgroup of $A_4$.

## Solution to Exercise E48

**(a)** The group $(\mathbb{Z}, +)$ is abelian, so all of its subgroups are normal, and hence in particular its subgroup $4\mathbb{Z}$ is normal.

**(b)** In any symmetry group, either all the symmetries are direct or half are direct and half are indirect, by Theorem B22. The regular tetrahedron has some indirect symmetries, such as the reflection in the plane that passes through two vertices and the midpoint of the edge joining the other two vertices, so half of its symmetries are direct and half are indirect. Hence the subgroup of direct symmetries of $S(\text{tet})$ is a subgroup of index 2, and therefore it is a normal subgroup.

**(c)** The 4-windmill has no indirect symmetries, so its subgroup of direct symmetries is equal to the whole group $S(\clubsuit)$ and hence is a normal subgroup.